

# **SAND REPORT**

SAND 2002-2566  
Unlimited Release  
Printed August/2002

## **Strategies for the War on Terrorism: Results of a Special Study**

The Advanced Concepts Group  
Sandia National Laboratories

Prepared by  
Sandia National Laboratories  
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,  
a Lockheed Martin Company, for the United States Department of  
Energy under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

**NOTICE:** This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from  
U.S. Department of Energy  
Office of Scientific and Technical Information  
P.O. Box 62  
Oak Ridge, TN 37831

Telephone: (865)576-8401  
Facsimile: (865)576-5728  
E-Mail: [reports@adonis.osti.gov](mailto:reports@adonis.osti.gov)  
Online ordering: <http://www.doe.gov/bridge>

Available to the public from  
U.S. Department of Commerce  
National Technical Information Service  
5285 Port Royal Rd  
Springfield, VA 22161

Telephone: (800)553-6847  
Facsimile: (703)605-6900  
E-Mail: [orders@ntis.fedworld.gov](mailto:orders@ntis.fedworld.gov)  
Online order: <http://www.ntis.gov/ordering.htm>



## Strategies for the War on Terrorism: Results of a Special Study

Advanced Concepts Group  
Sandia National Laboratories  
Albuquerque, NM  
June 2002

### **Abstract**

On September 13, 2001, the first day after the attacks of September 11 that Sandia National Laboratories re-opened, Vice President Gerry Yonas entirely redirected the efforts of his organization, the Advanced Concepts Group (ACG), to the problem of terrorism. For the next several weeks, the ACG focused on trying to better characterize the international terrorist threat and the vulnerabilities of the U.S. to further attacks. This work culminated in a presentation by Dr. Yonas to the Fall Leadership Focus meeting at Sandia National Laboratories on October 22.

Following that meeting, President and Lab Director, Paul Robinson, asked Dr. Yonas and the ACG to develop a long-term (3-5 year) technology roadmap showing how Sandia could direct efforts to making major contributions to the success of the nation's war on terrorism. The ACG effort would communicate with other Labs activities working on near-term responses to Federal calls for technological support.

The ACG study was conducted in two phases. The first, more exploratory, stage divided the terrorism challenge into three broad parts, each examined by a team that included both permanent ACG staff and part-time staff and consultants from other Sandia organizations. The "Red" team looked at the problems of finding and stopping terrorists before they strike (or strike again). The "Yellow" team studied the problems of protecting people and facilities from terrorist attacks, as well as those of responding to attacks that occur. The "Green" team attempted to understand the long-term, "root" causes of terrorism, and how technology might help ameliorate the conditions that lead people to support, or even become, terrorists. In addition, a "Purple" team worked with the other teams to provide an integrating vision for them all, to help make appropriate connections among them, and to see that they left no important gaps between them. The findings of these teams were presented to a broad representation of laboratory staff and management on January 3, 2002. From the many ideas explored by the Red, Green, and Yellow teams, and keeping in mind criteria formulated by the Purple team, the ACG assembled a set of five major technology development goals. These goals, if pursued, could lead to major contributions to the war on terrorism. With some rearrangement of team members and coordinators, a new set of teams began fleshing out these five "Big Hairy Audacious Goals" for the consideration of Laboratory leadership. Dr. Yonas briefed Sandia upper management on the work of these teams on February 4, 2002. This report presents the essence of that work as applicable to the R&D community of the nation interested in the development of better tools for a long term "War on Terrorism."



**INTRODUCTION OF THE PROBLEM**

THE NATURE OF THE THREAT..... 7  
STRATEGIES FOR DEALING WITH THE THREAT..... 8  
TRANSFORMATIONAL CAPABILITIES AND THE ROLE OF TECHNOLOGY ..... 12  
PURSUING BHAGS..... 15

**TALON—TERRORIST ACTIVITY LOCATION, OBSERVATION, AND NEUTRALIZATION . 18**

THE TALON APPROACH..... 19  
TECHNOLOGY CHALLENGES..... 23  
THE PATH FORWARD..... 25

**IRIS—INTELLIGENT ROBUST INFRASTRUCTURE SYSTEMS ..... 26**

AN EXAMPLE: AN AWARE AND ADAPTIVE CAMPUS ..... 28  
TECHNOLOGY CHALLENGES..... 30  
THE PATH FORWARD..... 34

**SSB—SECURE AND SMART BORDERS..... 36**

EXAMPLE OF SUCCESS..... 38  
TECHNOLOGY CHALLENGES..... 38  
THE PATH FORWARD..... 50

**FACETS—FRACTAL APPROACHES FOR CLARIFYING AND ENABLING TIMELY SUPPORT  
..... 51**

AN EXAMPLE OF THE BENEFITS OF A FACETS SYSTEM..... 55  
TECHNOLOGY CHALLENGES..... 58  
THE PATH FORWARD..... 58  
TECHNOLOGY CHALLENGES..... 65  
THE PATH FORWARD..... 66

**CONCLUSION ..... 67**

*THE SDAC (SENSE, DECIDE, ACT, COMMUNICATE) TEAM..... 67*  
*THE SSB (SMART SECURE BORDERS) TEAM..... 67*  
*THE FACETS (FRACTAL APPROACHES FOR CLARIFYING AND ENABLING TIMELY SUPPORT) TEAM ..... 67*  
*THE DICTUM (DYNAMIC INTEGRATED CAPABILITY FOR THREAT UNDERSTANDING AND MASTERY) TEAM... 68*



## INTRODUCTION OF THE PROBLEM

The diffuse nature, stealthy operation, fanatical motivations, and diversely destructive tactics of today's terrorists pose unfamiliar challenges to the United States. Countering the threats they pose will require a layered defense in depth, ranging from closing down the terrorists' sources of finance and recruits abroad, to finding and stopping them before they can attack, to mitigating the consequences of attacks we fail to stop. An effective layered defense, in turn, will entail the transformation of U.S. defensive capabilities for a new era.

### **The Terrorist Threat**

Today's terrorists can strike at any place, at any time, and with a wide variety of weapons. The most urgent terrorist threat to America is the al Qaeda network. We will prosecute our war with these terrorists until they are routed from the Earth. But we will not let our guard down after we defeat al Qaeda. The terrorist threat to America takes many forms, has many places to hide, and is often invisible. We can never be sure that we have defeated all of our terrorist enemies, and therefore we can never again allow ourselves to become overconfident about the security of our homeland.

President George W. Bush, *Securing the Homeland Strengthening the Nation* (Washington: The White House, February 2002)

The nation must learn to enable the many organizations involved in homeland and foreign defense to function as an integrated system. It must seek to deny terrorists the ability to hide their intentions and capabilities. Those with responsibility for defending the country must be provided with exquisite situational understanding of the threat environment. Since all threats cannot be preemptively stopped, the U.S. must find ways to "harden" its infrastructure and society against the most damaging potential effects of terrorist attacks. At home and abroad, law enforcement and military organs must be given the tools to deliver narrowly discriminating effects against diffuse targets. And all of this must be done in ways that preserve American values and constitutional protections.

### **The Nature of the Threat**

In the war against terrorism, the United States confronts an unfamiliar set of foes.

In the Cold War, it faced a superpower armed both with large conventional military forces and thousands of nuclear weapons. Mutual deterrence meant that the two fought only each other's proxies, while limiting the risks of direct confrontation with each other. In Iraq, superior U.S. conventional forces overwhelmed the ability of that nation to wage war with aircraft, armor, or troops.

In the war on terrorism, the conventional forces of nation states play only peripheral roles, and nation states themselves seek deniability for whatever support they provide to the terrorists. While some terrorist organizations are dedicated to nationalist causes, others see themselves as serving an ideological cause that transcends any national interests. With apocalyptic, transcendent beliefs, they can be difficult to understand, let alone

to deter.<sup>1</sup> They organize and operate by stealth in dozens of countries around the world. They may receive covert financial support from some nation-states, but they also receive sustenance from ideological sympathizers. Thanks to the vulnerabilities of modern technological society—as well as to the possibility that they will obtain weapons of mass destruction—their potential for inflicting human and economic damage is growing. And their goal of inflicting damage, mostly unrelated to any specific military objectives, makes the range of tactics available to them large, diverse, and unpredictable.

## Strategies For Dealing With The Threat

The Administration has not yet fully articulated its complete strategy against terrorism. The Office of Homeland Security has been charged with developing the aspects of that strategy that relate to the homeland, while the Departments of Defense and State are addressing the international aspects. Nevertheless, it is clear from the nature of the problem, and from the U.S. Government's response to it so far, that the U.S. defensive strategy must be multi-layered as well as multi-faceted. No one layer of defense can promise a high level of security against terrorism; multiple layers can make it increasingly difficult for terrorists to plan, organize, and carry out their deadly missions.

### *Layered Defense Concept*

The Advanced Concepts Group Special Study team began by considering the full range of measures that constitute a comprehensive layered defense. It did not expect to find that technology would have a major contribution to make to every layer, but it did believe that it was important to try to understand where technology contributions would fit into the larger strategic picture. We used a stop light analogy to describe our layered approach with the addition of a layer to ensure integration of the approaches in each layer. The basic elements of this approach are to find and stop terrorists, protect ourselves, respond to events that do occur, and address the root causes to prevent repetition of these events. These are depicted in the diagram below with more indepth discussion following.

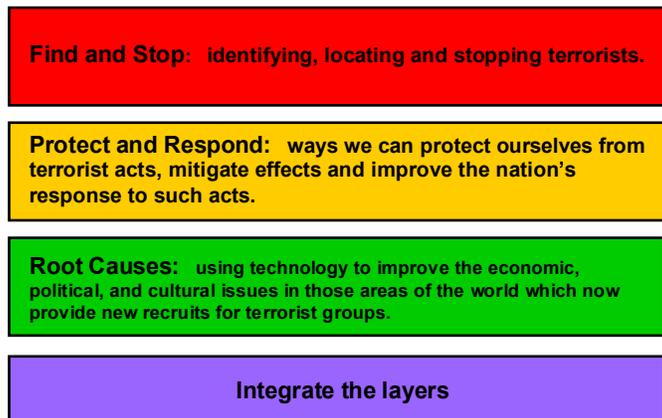
### **National Strategy for Homeland Security**

"The mission of the Office [of Homeland Security] shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."

President George W. Bush, Executive Order 13228, Section 2, October 8, 2001

---

<sup>1</sup> Cf. Roy F. Baumeister, *Evil: Inside Human Violence and Cruelty* (New York: W.H. Freeman, 1996).



### Root Causes

Terrorists begin as children or young adults who have not yet learned to see the targets of terrorism as enemies to be destroyed without mercy. At some point, they are recruited into the social and ideological milieu of terrorist beliefs and organization. Those already recruited to fanaticism are unlikely converts to peaceful paths of change. For those committed to martyrdom, no deterrent threat seems strong enough.

Still, it is at least possible to contemplate reducing the long-run recruitment pool for terrorist organizations. For example, improved economic opportunities in developing countries may give young people reason for hope and optimism, as opposed to despair and resentment against foreigners (the U.S. in particular) perceived as imposing economic and cultural oppression. We have seen in Pakistan that families with no other choice may send their children to fundamentalist schools where they are indoctrinated rather than educated. We have seen in Afghanistan that failed states can be co-opted by terrorist organizations, which use them as safe havens for the sheltering and training of terrorist recruits. These experiences suggest that foreign aid and “nation-building” could play a role in reducing the scale of the long-term terrorist threat.

Clearly U.S. foreign policy must not be dictated by terrorists. At the same time, in some cases, the United States might be freer to pursue its counter-terrorism interests if it were less constrained by such cross-pressures as dependence of the U.S. and its allies on international petroleum supplies. A frequently cited example is Saudi Arabia, whose government appears to have diverted domestic dissent away from its own shortcomings and toward religious and political hostility to the U.S. (Sixteen of the

September 11 terrorists were Saudi citizens, as once was Osama bin Laden.) The U.S. has long been deterred by its need for Saudi cooperation from pressing Saudi Arabia for democratic reforms.

Finally, although current terrorists seem undeterrable, it is conceivable that in the future we might come to better understand their thinking, motivation, and intentions so as to find ways to dissuade them from carrying out their plans, or at least identify and stop them sooner than is now possible.

### **Find and Stop**

If we cannot prevent foreign terrorist organizations from arising in the first place, we would next rather find them and stop them before they kill and destroy. One measure the U.S. has been taking is to trace and cut off the financial lines of supply to terrorist groups. This involves identifying front organizations, shutting down informal funds transfer systems, intercepting money-laundering schemes, and freezing bank accounts.

If terrorist organizations and cells can be discovered, there are ways to disrupt them. Some methods may include law enforcement measures (e.g., arresting members for terror- or non-terror-related crimes, expelling them, or returning them to other states where they may be facing criminal charges.) Other methods might be applied by intelligence organizations, such as infiltrating terrorist cells and sabotaging their activities, or finding ways of sowing dissension within cells or organizations.

Where terrorists have found sanctuary in weak, or even supportive, states, military action may be taken to capture or kill them. U.S. special operations forces are now working to train the Philippine military for this purpose. In Afghanistan, the U.S. took direct military action, but with special operations forces and standard military forces, to try to hunt down al Qaeda members. In addition, since the Taliban regime had allied itself with the al Qaeda, the U.S. used military force (cooperating with Afghani forces) to replace that regime.

### **Fire: An Analogy**

It is interesting to note that a little over 100 years ago our nation was in a similar position, faced with an unmanageable danger that threatened life and property and that was the source of significant dread for many people. In that case, the adversary was fire – a killer that could strike without warning. In addressing this threat, our nation developed a multi-faceted strategy that insinuated itself into many aspects of our daily life. While these encroachments may have seemed intrusive when first introduced, today they are commonplace, being barely noticed until needed. It is also interesting to note that we have not won “the war on fire.” Buildings still burn, property is still lost, and people still die. What has changed is that we now manage fire in ways that make it less likely to start, easier to contain, and, hopefully, less damaging when it does occur.

See the video, *An Analogy*, by Myra Edaburn and John Whitley, for more information on the parallels between our experiences with fire and with terrorism.

## **Protect and Respond**

If we cannot find and dismantle terrorist organizations abroad, then we would like our next layer of defense to prevent terrorists (and their weapons, if they are bringing them along) from entering our country. This means screening out bad actors and contraband through the processes by which we control our national borders. Should foreign terrorists penetrate our borders, we would like to find and arrest (or, at the very least, expel) them before they do any damage. If we cannot prevent them from acting, we can at least try to identify and ameliorate our vulnerabilities to terrorist attack. This may mean hardening our critical infrastructures (including information infrastructures) against the most debilitating threats. It may mean decoupling highly interdependent facilities to reduce the potential impact of attacks on one or a few of them. It may mean heightening the security of vehicles (e.g. large jets) or facilities (e.g. nuclear power plants) that could be turned into weapons.

Insofar as our targets can be made less vulnerable to massively destructive or disruptive attack, we may decrease the impact of attacks we cannot prevent. But we may also gain a measure of deterrence by making the terrorist’s mission seem too hard or too unpromising.

If all the other layers have failed, then at least we can be prepared for the worst in ways that minimize the direct and indirect costs of a successful attack. Part of that preparation will have been in the measures taken to reduce vulnerabilities. Part of it will be in the kind of responses we have planned to reduce and take care of casualties, to restore community social and economic life, and to rebuild what has been lost.

Finally, after terrorist crimes have been committed, we are back to finding and stopping those responsible before they kill again. The suicidal attacker has, of course, taken care of this himself. But if those who directed, sponsored, or supported the attack can also be neutralized, then both the prevention and the deterrence of future attacks will be served.

It is obvious that these layers of defense against terrorism are not purely—or even mostly—technological in character. They will result from a complex synthesis of political leadership, government policies and actions, (from municipal to federal, and with considerable international cooperation as well), private and public organizational behavior, and citizen support. Technology can offer tools—sometimes very powerful tools—but not the

human will and capacity to use the tools wisely and effectively. We now turn to how technology can help.

## **Transformational Capabilities and the Role of Technology**

The layers of defense against terrorism cannot simply be divided up amongst different government agencies and administered independently of each other. Nor are all the tools that now exist for protecting U.S. domestic and international security perfectly adapted to the unfamiliar nature of the threat. The U.S. effort against terrorism will best be served by the transformation of our defensive capabilities to match the problem. Following are some “transformational capabilities” that would better position the U.S. to cope with the terrorist threat, along with some indications of how technology could help.

### *Enable Stovepipes to Function as a System*

The multi-layered, multi-faceted nature of the terrorist threat calls for a national response in which the collection of capabilities—international, military, federal, state, local, and private—operates as if it were a well-tuned system-of-systems. Much of our inability to achieve joint, seamless operations is due to political, bureaucratic, and budgetary stovepiping. But technologies can play a role in helping the many organizations involved in homeland defense to overcome the barriers to communication and coordination. Technologies could:

- enable common perceptions of operational priorities and objectives,
- minimize incompatibilities between various tools and techniques,
- integrate information from diverse sources,
- provide the most appropriate portals of understanding for diverse operational communities,
- offer exquisite C<sup>3</sup> (Command, Control, and Communications) connectivity, and
- support training in ways that are palatable for each community.

Technologies offering these capabilities will not substitute for leadership and organizational innovation. But they could demonstrate the feasibility and value of a new level of joint operation amongst diverse governmental and private organizations.

### *Deny the Ability of Adversaries to Hide Intentions and Capabilities*

Our deterrence of current terrorists could be greatly strengthened by capabilities to extensively and rapidly collect, integrate, analyze, and apply forensic information from across all phases of attacks (pre-, trans-, and post-). This would need to be done in a manner that conveys assurance that perpetrators will be unmasked, and increases the expectation of doing so more quickly and in earlier phases than today. Technologies may help provide:

- more extensive surveillance of potential indicators and perpetrators,;
- rapid collection of potentially incriminating information,
- ongoing analysis to rapidly discern potentially incriminating patterns,
- rapid dissemination of warning or discovery to appropriate intelligence, law enforcement, military, or other government bodies worldwide, and
- appropriate protection of constitutional rights, need to know, transparency, and accountability.

### *Provide Exquisite Situational Understanding*

An accurate, relevant understanding of what is happening would be invaluable to everyone who must cope with terrorism, from the President, to the soldier in the battlefield, to the customs and INS officials trying to protect our borders, to the FBI agents hunting down terrorist cells, to first-responders and local officials reacting to an attack, to individual citizens. Exquisite situational understanding might be enabled by technologies that:

- monitor all available relevant information sources,
- collect reliable, accurate information on conditions that range from imperceptible to chaotic,
- integrate it in a manner that provides the fullest possible recognition of current conditions,
- project it forward to anticipate how conditions might develop,
- assess the impacts of mitigating responses, and
- convey understanding appropriate for various levels of decision-making.

### *Harden the Homeland*

For the foreseeable future, it is implausible to imagine that all attacks with massively disruptive potential can be deterred, prevented or interdicted. The prospect for such attacks will be part of the “background” of risks that need to be managed in

order to provide for reasonable safety and conduct of society. But defensive measures can help ‘harden’ society against the damaging effects of terrorist attacks. These include both responsive measures that are initiated after an event is detected, as well as precautionary measures that raise damage thresholds and facilitate recovery. These defensive systems will be implemented and operated by a mix of stakeholders that range from Federal agencies to individual citizens.

Many options are currently available, and many more being developed, for increasing the hardness of domestic assets. Technology can help develop and demonstrate cost-effective means, architectures, and approaches for transforming U.S. society into an intrinsically harder target.

#### *Deliver Discriminating Effects against Diffuse Targets*

Terrorists will be unpredictable and diffusely distributed, often among non-combatant populations or in access-restricted locales. Their supporting infrastructure and operations (recruitment, training, RDT&A, financial, logistics, C<sup>3</sup>I, etc.) will often utilize otherwise legitimate societal activities and functions. Their cohorts and supporters will often be interspersed among general populations or otherwise legitimate, perhaps sacrosanct, enclaves. Such diffusion offers not only covert for threats, but also sanctuary in which those disaffected with the U.S. can be indoctrinated, trained, and sheltered. Collateral damage and unintended consequences from insufficiently discriminating U.S. actions against diffuse threats can provide powerful weapons for terrorist psychological operations. Imprecise applications of force place our own and allied soldiers at risk.

This challenging threat landscape would be transformed by U.S. capabilities to precisely discriminate, designate, and neutralize diffuse targets while absolutely minimizing collateral damage and unintended consequences. Such interdiction capabilities are needed for a broad range of tactical targets (e.g. urban combatants, sheltered equipment, usurped communications assets) and strategic targets (e.g. leadership, financial networks, extremist cells, WMD capabilities, supporter networks, logistic resources). The approaches used must span, and in some cases simultaneously blend, the operations of military, law enforcement, intelligence, and perhaps other domains.

## **Pursuing BHAGs**

In attempting to outline a set of research programs by which the nation's technology providers could contribute in a major way to the war on terrorism, the study team adopted the "Big, Hairy, Audacious Goal (BHAG)" concept advocated by Collins and Porras.<sup>2</sup> A BHAG is a large, long-term goal that can provide inspirational vision. The BHAGs suggested in this paper are also of such scale as to require strong partnerships among research institutions, industry, and the government customers who must buy and use them. They do not purport to solve every problem at every level of defense against terrorism, but in many cases they would supply capabilities that would be valuable at more than one level.

### *TALON: Target Acquisition, Location, Observation And Neutralization*

This BHAG aims to help transform U.S. military capabilities to enhance situational awareness and precision attack against diffuse and hard-to-kill targets. It envisions development of integrated systems that combine smart, virtually ubiquitous, persistent observation with precision engagement. These systems would find, characterize, and discriminate terrorist targets, then support or execute interdiction. They would utilize networked arrays of fixed and mobile platforms that can Sense, Decide, Act, and Communicate (SDAC) with collective intelligence and autonomy.

### *IRIS: Intelligent Robust Infrastructure Systems*

Defending the U.S. homeland against terrorist attack is an enormous undertaking. As an alternative the guards and guns strategy typical of our response to 9/11, the "Intelligent Robust Infrastructure Systems" (IRIS) BHAG proposes a three-pronged approach to protecting our infrastructures. First, build things "hard" from the start and, where critical, retrofit existing entities to make them resistant to catastrophic failure. Second, make "things" aware and adaptive so that they intelligently and autonomously respond to events in their environment, where appropriate, and, when human intervention is required, can inform and protect the first responders. Finally, make it easy to rapidly reconstitute infrastructures when they are damaged in an attack.

---

<sup>2</sup> James C. Collins and Jerry I. Porras, *Built to Last: Successful Habits of Visionary Companies* (New York: HarperBusiness, 1997).

### *SSB: Secure and Smart Borders*

The challenge in border management is to maintain the smooth flow of commerce and legitimate travel, but at the same time increase the probability of screening out bad actors and contraband. SSB envisions a border management architecture for the U.S. that encompasses not just the geographic and political boundaries, but portals and perimeters at all levels. A flexible and adaptive border security system would use SDAC assets in a layered approach. For example, cargo and visitors may be more efficiently screened and certified as safe before they even leave their cities or countries or origin. The envisioned architecture employs sensors, information technology, procedures, and human decision makers in a seamless manner that enhances the flow of legitimate traffic while increasing scrutiny of potentially dangerous targets.

### *FACETS: Fractal Approaches for Clarifying and Enabling Timely Support*

The first responders to an act of terrorism in the U.S. are local emergency response and law enforcement personnel, the organizations they serve, and the local governments of jurisdiction. In addition, over time, state governments and dozens of Federal agencies have various responsibilities for helping cope with the emergency. How could all these planners, decision-makers, and responders be provided with a common situational understanding and ability to see, decide, act, and communicate in more seamless, agile, timely ways than are now possible? The FACETS concept envisions a fractal SDAC architecture that permits rapid situational understanding and dynamic response by all the relevant parties. This fractal response architecture would:

- overarch the various units of emergency response,
- require some common functionality,
- define interfaces,
- provide a system that scales easily,
- be easy to use (“plug and play”), and
- be able to reorganize adaptively.

### *DICTUM: Dynamic, Integrated Capability for Threat Understanding and Management*

DICTUM is the goal of understanding terrorists so well that intelligence, military, and law enforcement officials could match indicators to activities before attacks took place, anticipate enemy capabilities and actions, and know how to influence

terrorist processes. This understanding would be advanced by developing information technology-based tools for better threat assessment and management. Those tools would be based on multi-disciplinary conceptual models of terrorist organizations, capabilities and intentions.

### *About this Report*

Each of the following sections discusses one of these BHAGs in greater detail. For each BHAG there is a fuller explanation of what its accomplishment would look like and how it would contribute to winning the war against terrorism. An example of how the proposed set of capabilities might apply to a specific situation is given. Each BHAG is broken down into subsets of technology challenges. Some path forward is suggested for these lines of technology development.

Two additional observations about the entire set of BHAGs are in order. First, at some point each calls for new tools that perform advanced functions similar to those performed by humans—tools with abilities to see, decide, act and communicate. While, at times, these proposals may sound like call for replacing humans with technology, that is not the intent. Instead, the goal is to develop tools that help humans do what they do more quickly and effectively. In some cases, this will mean permitting machines to take important—but not irrevocable—actions within shorter periods of time than humans can act. But in many other cases, by increasing sensing, information access, and communications capabilities, the tools will empower humans to make better decisions and cooperate more effectively with one another. The central theme of the BHAGs, then, is to find the most effective combinations of human actors and technology tools.

A second observation is that the BHAGs all imply human-technology systems that are constantly learning and adapting to changing environments. This will require systems that not only react to feedback from the environment, but that have built-in mechanisms—red teams in one form or another—for continuous self-testing and re-evaluation. This characteristic is essential to keep the systems aware and responsive when the real threats materialize only infrequently, but are have catastrophic effects when they do.

## TALON—TERRORIST ACTIVITY LOCATION, OBSERVATION, AND NEUTRALIZATION

Dedicated, ruthless, and suicidal terrorist individuals and organizations have demonstrated escalating capability and willingness to inflict thousands of civilian deaths and injuries, billions of dollars in economic losses, and social upheaval. A sequence of such events, or even more severe attacks involving chemical, biological, or nuclear weapons of mass destruction (WMD) could bring about extreme national crises.

Today's terrorist threat involves small numbers of highly motivated and well-financed agents diffusely embedded within local societies, both domestic and foreign. They are typically affiliated through loosely knit, like-minded organizations and support networks. The attack of September 11 demonstrated a new level of this asymmetric threat to which the U.S. is vulnerable. Defensive security and emergency response measures are important but not sufficient to deal effectively with this threat. More timely, agile, and precise "Find and Stop" offensive capabilities are also needed.

*Terrorist Activity Location, Observation, and Neutralization* (TALON) represents a specific "Find and Stop" task focus within the broader scope of the strategies for the War on Terrorism outlined earlier. TALON explores system approaches for providing more timely and effective threat detection and offensive neutralization capabilities to prevent or thwart high-consequence terrorist attacks.

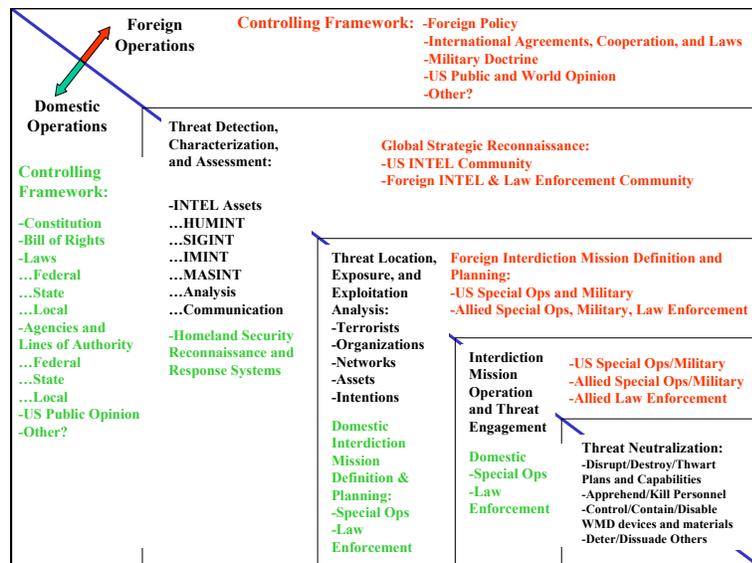
The counter-terrorism effort confronts complex and often conflicting challenges, ranging from the need for improved intelligence information collection, analysis, and sharing across stovepiped organizational boundaries to legitimate concerns about the preservation of civil liberties, personal privacy, and fair treatment of individuals within our constitutional and legal framework. Technology-based system solutions are essential for improving our national capabilities for dealing with the terrorist threat.

The nation needs to be able to engage, dominate, and win against terrorists through the prevention of high-consequence attacks and the reduction or removal of specifically identified threats by offensive actions. We also need to be able to neutralize terrorist threats by removing the ability or desire of terrorists to carry out attacks through

- dissuasion, disarmament, apprehension, or killing of individual terrorists,
- disruption of terrorist operations,
- denial of access to needed finances, materials, sanctuary, training, etc., and
- disablement, containment, and safe disposal of weapons and materials of mass destruction (WMD).

## The TALON Approach

Successful terrorist attacks against U.S. property and personnel abroad had been a recurring problem before September 11. The intelligence community had issued warnings of possible homeland attacks for some time and, fortunately, had been able to thwart numerous attempts in recent years. Nevertheless, national capabilities and support systems still lack the agility needed to detect, locate, communicate, and prevent impending attacks by organized and determined terrorists.



The initial phase of the U.S. War on Terrorism has successfully removed the Taliban from power and disrupted high-level operations of the al Qaeda terrorist organization, but it has not yet resulted in the definitive removal of key leaders, including Osama bin Laden. Moreover, significant threats remain from diffusely distributed terrorist cells and individuals around the world. Such threats are embedded within local host societies, including the U.S.

On the “find” side, improvements are needed in the areas of threat detection, characterization, identification, precise

location, and tracking. Specific counter-terrorism targets include terrorist individuals, organizations, activities, assets, and support capabilities and infrastructure. On the complementary “stop” side, improvement is needed in the capability to accurately discern and quickly neutralize (with minimal risk to operational personnel and little or no collateral damage) identified terrorist threats and associated means of mass destruction before attacks can be carried out.

Effectively finding and stopping terrorist threats demands technical and operational improvement and coordination among a broad range of reconnaissance, detection, surveillance, intelligence, and precision engagement assets and organizational capabilities that collectively enable threat identification and neutralization. Foreign operations are also governed by international agreements and cooperation with allied government, military, and law enforcement agencies.

The essence of the problem is to disable or destroy terrorist organizations, individuals, or their enabling assets and capabilities, by precisely delivering neutralizing actions. First, however, we must locate and identify terrorists, their activities, or their enabling assets, capabilities, and support infrastructure—at home or abroad—before they can initiate or complete high-consequence acts of terror. This ultimately demands substantial improvement in the provision of human intelligence, appropriately shared and combined with other timely information, distilled and shared from disparate sources. In sum, we need transformational capabilities that will produce exquisite intelligence for precision strike.

We face the following obstacles to achieving exquisite intelligence and precise action for finding and stopping terrorists.

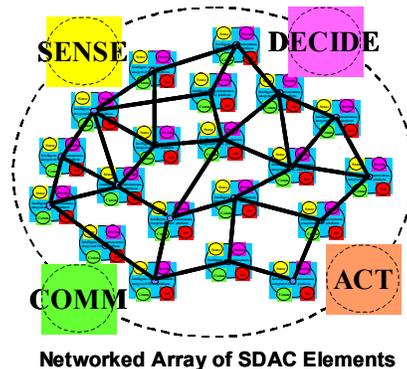
- Terrorism is both a domestic and international problem, requiring information flow, cooperation, coordination, and collaboration among many organizations, lines of authority, and their associated conflicting interests and agendas.
- One faction’s “Terrorist” may be another faction’s “Freedom Fighter”...making cooperative coalition building and consensus more difficult to achieve.
- Terrorist organizations and individuals are often idealistic, diffusely distributed, compartmentalized, and embedded within local civilian societies ... making infiltration and activity detection more difficult, and increasing collateral damage risk from direct engagement with lethal force.

“Exquisite intelligence on the intentions and capabilities of adversaries can permit timely adjustments to the force and improve the precision with which it can strike and defend.”

Donald Rumsfeld, *Nuclear Posture Review* (January 3, 2002)

- Detecting and neutralizing terrorists is heavily dependent on INTEL (particularly HUMINT, based on past experience).
- INTEL community is secretive, fragmented, turf-sensitive, less-than-agile, and currently lacking in international anti-terrorism HUMINT capabilities in key areas.
- Close communications and coordination among disparate INTEL, Military Operations, Law Enforcement, and other organizations is lacking due to stove-piped organizational structures, organizational culture differences, technical incompatibilities, lines of authority, and access control issues.
- Domestic operations and techniques are constrained by constitution, laws, etc.
- Foreign operations and techniques are constrained by international cooperation, laws, policies, host country sensitivities, or logistics.

## Terrorist Activity Location, Observation and Neutralization (TALON)



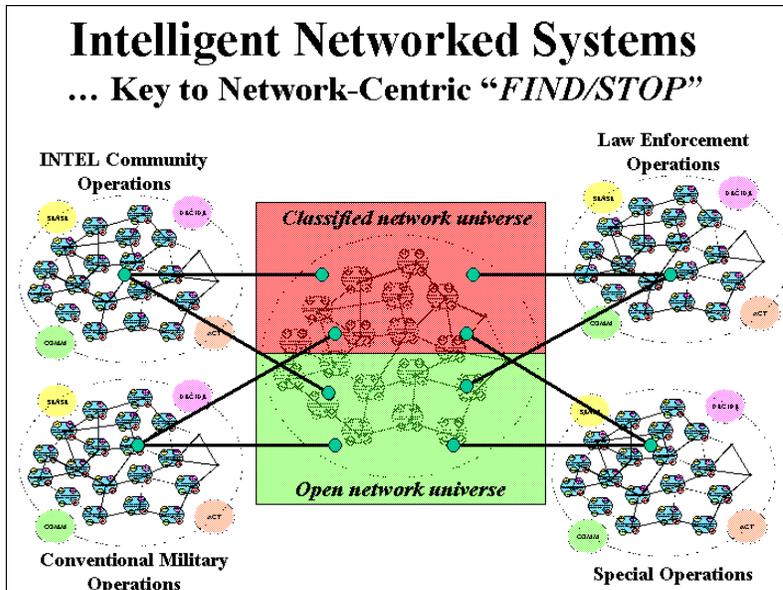
### The development of integrated systems:

- that utilize networked arrays of fixed and mobile sensor/responder (SDAC) platforms
- which Sense, Decide, Act, and Communicate with collective intelligence and autonomy
- to find, characterize, and discriminate terrorist targets, and
- to support or provide interdiction capabilities

Smart, Ubiquitous, and Persistent Observation w/ Precision Engagement

The TALON study has identified *Intelligent, Networked, Sense, Decide, Act, and Communicate (SDAC) Systems* as essential to an agile, information-rich enterprise required to “Find and Stop” terrorist threats.

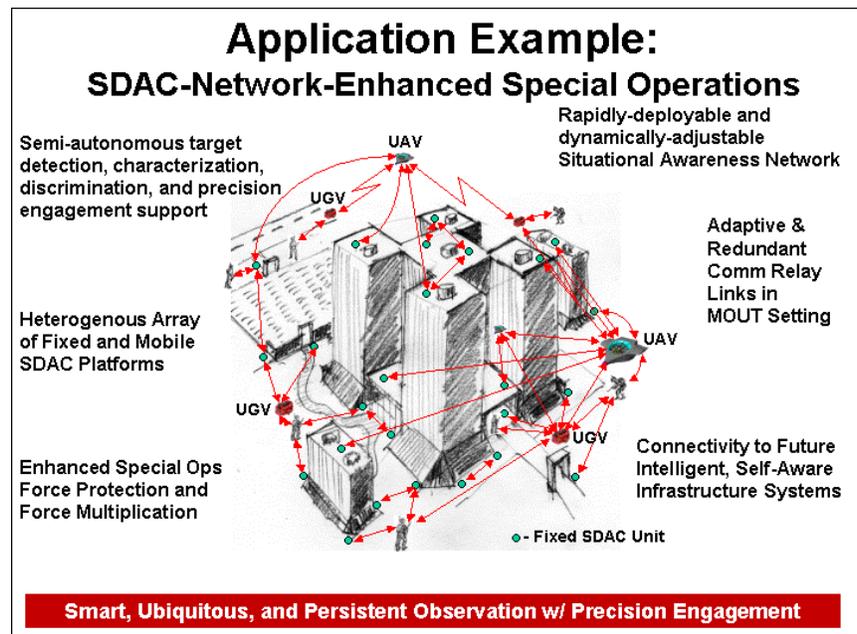
Smart, networked SDACs represent a new class of technology-based systems with adaptable recognition and decision-making (cognitive) functionality, and such systems offer revolutionary transformational capabilities for providing timely intelligence information, situational awareness, portal/border monitoring, critical infrastructure monitoring, law enforcement and military operations support, and other applications critical to homeland defense and the global WOT.



The “nodes” within a networked SDAC array consist of individual systems each consisting of a suite of sensors, power system, on-board processing, command, and control, communications, a deployment platform or housing, and the ability to take action. Deployment platforms for individual SDAC systems may be fixed or mobile, and they may be packaged for low-observable covert operations or for more open applications. System actions can range from simply communicating information, to relocating (in the case of mobile platforms), to designating targets or directly activating weapons systems (non-lethal or lethal) against identified targets. Other specialized actions could include the remote deactivation or containment of explosive devices or dangerous materials.

A specific example application is support of Special Operations (SO) in urban terrain is depicted in the figure below. The SDAC array consists of a mix of fixed and mobile platforms (unmanned ground and air vehicles), with networked communications among the SDAC elements and with SO personnel. The small, fixed elements depicted could be lower-capability units

deployed by hand or by airdrop. The higher-capability, unmanned mobile vehicles could be brought in by transport vehicle and deployed at the boundary of operations. The combination of fixed and mobile SDAC elements of varying capability in a networked configuration provides dynamic spatial adjustment capability for improving situational awareness and adapting to changing operational conditions. Other applications examples include networked arrays of trail-monitoring systems, networked arrays of monitoring systems for border/perimeter/portal/critical-infrastructure applications.

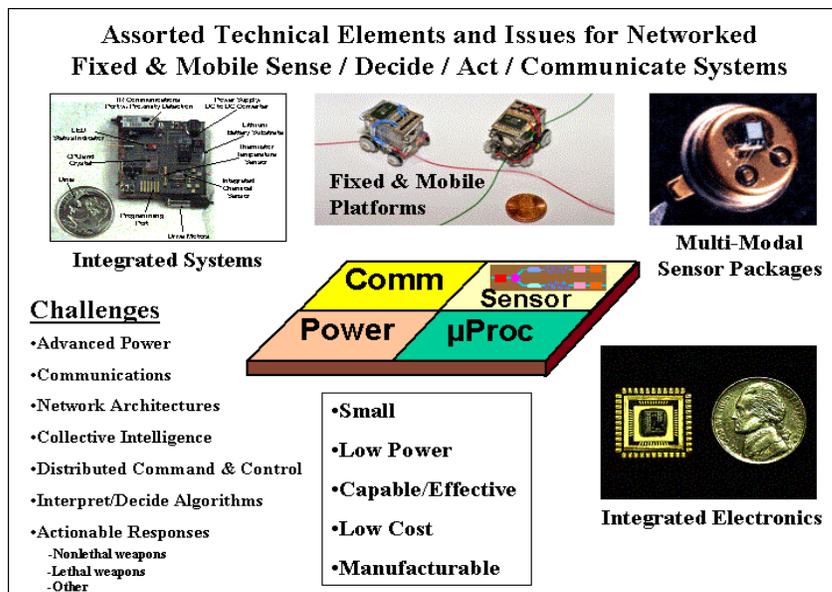


## Technology Challenges

The challenge will be to design, model/simulate, develop, implement, test, and demonstrate a smart adaptable sensor array capable of detecting, locating, identifying, reporting, and taking action against target. The elements and features needed are:

- Large networked semi-autonomous array of smart sensor systems (SDACs) that each sense, process, make decisions, act, and communicate information
- Combination of fixed and mobile sensor platforms (ground/air)
- Small, cheap SDACs easily deployed by air or ground personnel; some SDACs more capable (e.g. mobile) and expensive.

- Collective intelligence and adaptability with semi-autonomous sense/decide/act/communicate (SDAC) capabilities
- Enhanced situational awareness and support for interdiction “actions”
- “Arsenal” of actions may include the ability to disrupt or disable weapons (non-lethal, lethal)
- Desired operational capabilities:
  - detection and characterization of people, vehicle traffic, objects, and facilities;
  - networked and capable of semi-autonomous operations;
  - detection, identification, designation, and notification of targets for precision strike; and,
  - actions for disruption or disablement.

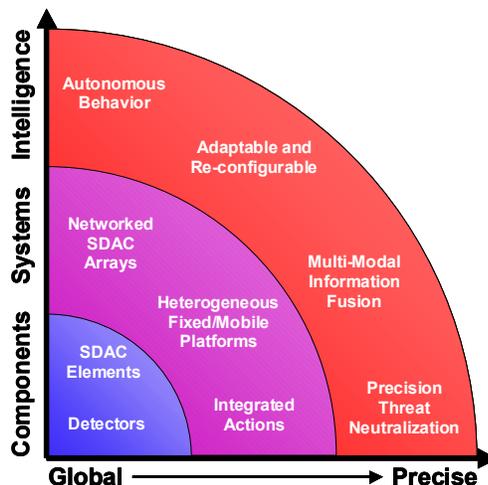


The technical solutions needed to successfully design, develop, and implement networked SDAC array systems for selected applications involve many disciplines. Engineering tradeoffs must be made among numerous system parameters and performance requirements, which will depend strongly on the specific application scenario. The general goal is systems that are smaller, lighter, cheaper, with lower power consumption, longer operational life in the field, and greater functional capability than are now available. Practical systems obviously require making compromises dictated by the state and maturity of enabling technology development and the realities of the application and use scenarios.

Producing the desired systems will require a combination of enabling technology advancement with focused applications engineering design, development, packaging, integration, and test/evaluation. Meeting the challenges can be realized through the full engagement of:

- **modeling and simulation community** to provide insights for systems design and operational capability tradeoff studies;
- **engineering and electronics establishment** to focus on key technologies that underlie smaller, lighter, lower power sensor, communications and mobile platforms for these systems;
- **assisted target recognition, information fusion/exploitation, cognition, and collective intelligence community** to broaden the scope of system architecture and algorithm R&D to radically improve capabilities for embedded intelligence, recognition, situational awareness, and autonomous decision-making;
- **energy storage and collection technologies** to develop smaller, lighter, higher energy density energy storage devices and power systems;
- **explosives and directed energy communities** to develop ‘interesting’ lethal and non-lethal devices and systems;
- **community of communications experts** to develop *sensor-web-enabling* communications architectures and systems;
- **systems engineering** to define integrated systems concepts, architectures appropriate for addressing critical customer needs and use scenarios;
- **manufacturing technology** to identify the most appropriate approaches for cost-effective manufacturability; and
- **sensors** to envision radical transduction schemes and mechanisms.

### The Path Forward



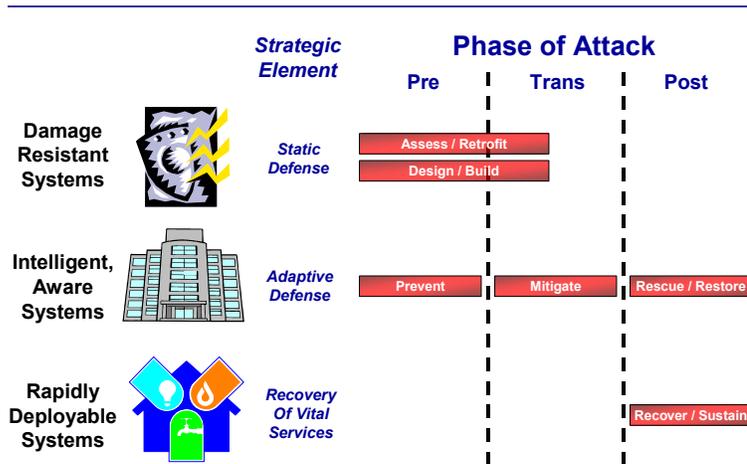
We should pursue this work in two directions

- Increasing Collective Systems Capability & Intelligence
- Increasing Operational Precision

## IRIS—INTELLIGENT ROBUST INFRASTRUCTURE SYSTEMS

Defending the U.S. homeland against terrorist attack is an enormous undertaking. While we might be willing to pay the \$2-3 billion required to federalize security at every domestic airport and can pour \$6 million into security for the Super Bowl and \$300 million into protecting the Olympics, can we do this for all vulnerable points in the nation? And even if we could, would we really want to? Clearly the answer is “no.” We are “the land of the free,” not “the land of the security checkpoint.”

As an alternative the guards and guns strategy typical of our response to 9/11, the “Intelligent Robust Infrastructure Systems” (IRIS) BHAG proposes a three-pronged approach to protecting our infrastructures (see figure below). First, build things “hard” from the start (and, where critical, retrofit existing entities to make them resistant to catastrophic failure). Second, make “things” aware and adaptive so that they intelligently and autonomously respond to events in their environment, where appropriate, and, when human intervention is required, can inform and protect the first responders. Finally, make it easy to rapidly reconstitute infrastructures when they are damaged in an attack.



### The Robust Infrastructures Strategy

The first prong of this strategy addresses two needs: what to do for existing systems and what to do for systems that are still in the process of being designed and built. For existing systems, we need ways of identifying which assets are the most important to

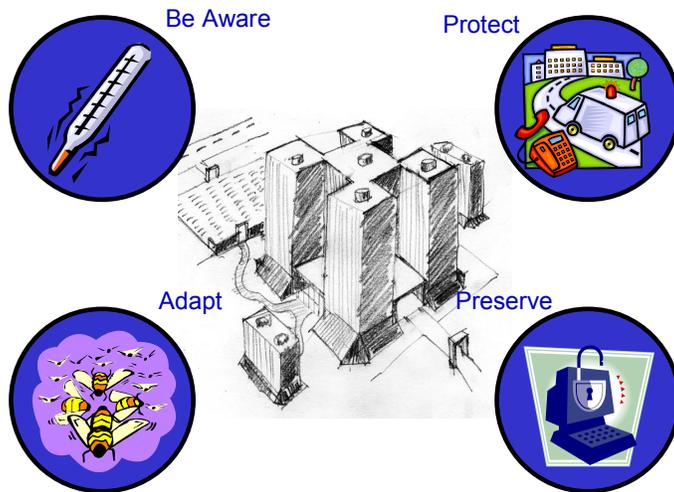
harden and mechanisms for evaluating the relative effectiveness of the potential hardening strategies. In as much as ownership of this problem is shared across the government and private sectors, we must figure out how to make the knowledge and tools used by the experts accessible such that users and owners of a wide range of systems and structures can address their own needs in this area. On the design side, we require new design approaches that account for active threats and that allow us to affordably harden the things that we produce and we need new methods and materials to support the implementation of systems designed with these approaches.

The second prong of this strategy focuses on creating systems that can adapt to changing threat environments. The goal is to create systems that autonomously act, where appropriate, to preserve the functions that they support and to protect the people who depend on these systems and that work with first responders, when they are needed, in ways that make the responders more effective. For example, an “aware” World Trade Center complex could have alerted rescuers to the imminent collapse of its towers. An intelligent Hart Office Building could have identified the presence of anthrax and then acted to contain the bio-agent and to identify individuals likely to have been exposed. Similarly, large-scale computer networks might be vested with knowledge of themselves and of the reason for which they exist. With this insight and the proper intelligence, they can adapt to detected threats and continue to operate through attacks while, at the same time, acting to isolate affected systems, terminate the attacks, and then reconstitute. Local power grids or water systems could be made smart enough to assess their own state of health after attack and to automatically recover as much of their capability as possible. Common spaces (e.g., passenger compartments of planes, stadiums, and lobbies of buildings) could detect people who pose potential threats and act to protect others in the space.

The final prong of the strategy acknowledges the fact that perfect protection is never possible—the attacker always has the advantage. While you can make his task more difficult or his attacks less effective, you will never be able to stop him completely. Given this, the U.S. strategy for infrastructure protection must include approaches for rapidly restoring, on an interim and permanent basis, access to vital services—power, communication, water, waste treatment, healthcare, and security—lost in an attack.

## An Example: An Aware and Adaptive Campus

To understand how this strategy might express itself in a real-world setting, consider a “smart campus” (as shown in the figure below) consisting of several buildings, ground-level and underground parking, subway access to the property at the lowest level of the parking structure, and walking paths and seating areas scattered throughout the grounds.



### *Build It Hard*

From the start, the campus’ physical structures were designed with safety, security, and survivability in mind. The architectural and engineering tools used in designing the campus ensured and the methods and materials used during its construction all presumed the need to address threats from an active adversary. As a result, the building is highly resistant to catastrophic failure. The design of the campus structures allows multiple escape paths from most points within the structures. The main systems (power, communications, HVAC, water) are engineered to allow for rapid isolation of different subsystems and the automatic rerouting of services to unaffected portions of the structures. Traditionally vulnerable points of the structures, such as the shipping and receiving area, are designed for containment of explosives and contaminants.

### *Make It Aware of Itself*

Each of the structures on the campus is endowed with a “deep” self-awareness through a combination of rich instrumentation and detailed models of “self” that allow for reasoning about the structures’ present state and possible future states. In addition to

knowing itself, each structure on the campus has an understanding of its internal and external environments, of the people and things that occupy the structure, and of the significance of each of these things.

*Make It Aware Of Its World and Its World Aware Of It*

In addition to the self-awareness of individual structures, the campus as a whole possesses a collective awareness that permits events of importance to the campus community to be known by all structures on the campus even if perceived only by one of the structures. Likewise, the campus itself shares a collective awareness with other structures in its immediate neighborhood, in the city of which it is a part, and, for some elements, even in the region and nation to which it belongs. This collective sharing at all levels makes it possible for the structures within the collective to maintain a broad awareness of potential threats and to intelligently plan for and respond to these threats as they unfold.

*Enable Autonomous Response When Appropriate*

Campus structures are able to handle autonomously many situations that might arise on campus. The campus as a whole identifies and attempts to characterize every individual and vehicle entering the campus. For each such entity, the campus can develop an appropriate level of “paranoia”, focusing more attention on those perceived as potential threats. Locks on doors operate automatically to allow trusted parties to enter various areas of the campus and to bar entry to untrusted individuals. Detection of dangerous agents (e.g., chemicals or certain biological substances) is handled by isolation and building-mediated evacuation. Loss of certain services (e.g., the cutting of a network cable) is detected and automatically accommodated through rerouting of services and, if needed, interactive rationing of bandwidth to affected clients. People who pose an immediate threat to building occupants may be deterred or incapacitated through the use of “soft stop” technologies.

*Promote Effective Human Response*

In situations where response is beyond the ability of the campus structures to handle, the structures are able to marshal the services of both campus tenants (e.g., for immediate response to a heart attack) and “professional” first responders. In the case of the first, the structures are aware of the abilities of each of its tenants (e.g., “Joe in XYZ Corp is EMT certified”) and may

have even participated in the equipping of many of these tenants (e.g., “emergency response captains” on each floor of a building might be trained by the campus using scenario simulations). In the case of the second, the campus shares its awareness with the first responders to allow these professionals to assess the situation on the campus, to explore in real-time various avenues of attack, and to begin to take steps to manage the situation even before they reach the campus. Upon arrival, the campus provides the responders with access to its communications infrastructures to augment the responders’ ability to communicate with each other and with tenants who need their assistance and to permit them fuller access to the control of critical campus subsystems.

### *Support Rapidly Recovery of Vital Services*

In the wake of an attack that damages campus structures, the campus assesses its own state of health and participates in planning how to reconstitute campus services. In addition, the design of the campus allows for “drop-in-place” infrastructure components (e.g., communication gateways for connecting the campus to the outside world, mobile waste handling systems, “instant” perimeter security systems, or “personal” power sources for providing essential power to individual apartments or offices) that support rapid reconstitution of essential services.

## **Technology Challenges**

The challenges encountered in realizing this vision are significant. They include:

- **off-line and real-time modeling and assessment of large-scale, complex systems** – the underlying science in this area is immature; we don’t know how to create models that faithfully capture the richness of real-world systems; we don’t know how to assess these systems in “whole system” fashion during their design; we don’t know how to enable the systems to assess themselves in real-time once in the field
- **methods and building blocks for the implementation of sure systems** – engineering history is replete with examples of good design being undermined by poor implementation and, in many engineering disciplines, we lack both the tools and raw materials needed ensure the faithful rendering of sure designs as well as the means to assess after the fact whether as-built systems matches their designs
- **affordable, “broad spectrum”, ubiquitous monitoring** – a system’s “self-awareness” is predicated on its ability to

perceive; however, fielding large-scale sensor systems that monitor a wide range of phenomena and effectively integrate data to develop rich pictures of the physical worlds that they watch is currently beyond engineering's abilities

- **tools for endowing “things” with the ability to respond autonomously** – it is one thing to endow systems with the ability to sense and reason about themselves and their environment and another altogether to give them the ability to respond to changes, especially in “high consequence” environments
- **secure, distributed, collaborative computing** – these environments, based on very large numbers of dynamically federating, intelligent nodes communicating over capable networks, will require new architectural approaches to distributed computing
- **effective computer-human interaction** – if these systems are to protect their human users in a range of situations, then they must be able to “understand” and collaborate with the humans in their environment; this includes being able to not only identify individuals and groups but to also characterize what and how they are doing, as well as being able to effectively communicate with individuals, tasks that are currently beyond us
- **privacy and anonymity** – we lack the means for protecting users in a fully “wired” monitoring-intensive world against misuse of information gathered; mechanisms for addressing the imbalance between the observers and the observed are needed
- **sustainable mechanisms for recovery of vital services** – recovering lost services presents emergency management personnel with a number of challenges: rapidly assessing damage and restoring viable infrastructures to service, quickly patching in new infrastructure elements when the demand for them is potentially large and widespread, controlling demand so as to conserve resources, and monitoring the health of this patchworked infrastructure and that of the people it serves for emergent problems.

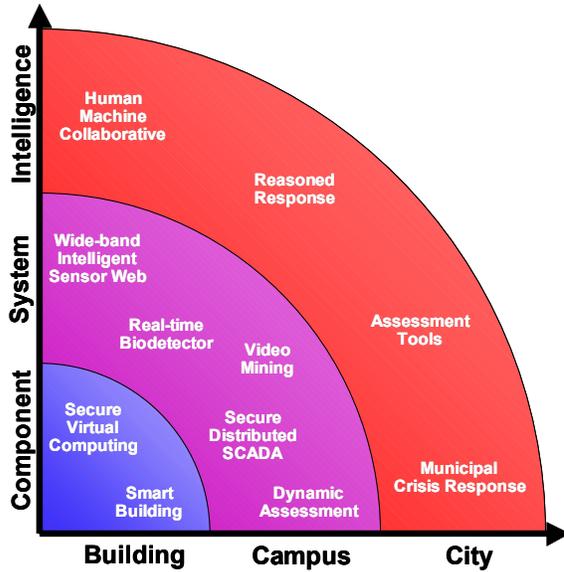
For each of these challenges, the following table identifies specific needs that, if addressed, would help satisfy the challenge.

Challenge	Needs
Modeling and Assessment of Large-Scale Complex Systems	<p>“Fourth generation of assessment science” where the focus is on real-time assessment of large-scale, complex systems and where the assessment is done by the systems themselves</p> <p>The incorporation into this science of methods for addressing the active threat agent</p> <p>Tools that make this science accessible to a collection of users whose knowledge and skills in this area may vary widely</p> <p>Methods of rapidly developing the models that drive these assessments</p> <p>Computing frameworks that allow us to endow systems the ability to reason based on these fourth generation approaches.</p>
Methods and Building Blocks for Sure Systems	<p>Sure implementation methods in a range of disciplines</p> <p>The development of building blocks (construction materials, source code, etc.) from which these sure systems can be built</p> <p>Means of providing inspectors of systems with ways of determining that sure designs have been faithfully implemented and that the integrity of the materials used in implementation have not be compromised.</p>
Affordable, “Broad Spectrum”, Ubiquitous Monitoring	<p>Suites of sensors that are small and cheap enough to deploy widely and deliver a broader range of sensing modalities</p> <p>Approaches for fusing data streams from diffuse sources into a rich, coherent picture of “ground truth”</p> <p>Architectures for seamlessly stitch these devices into the secure, distributed computing environments that they support.</p>
Tools for Endowing Things with the Ability to Respond Autonomously	<p>Planning systems appropriate to complex environments</p> <p>Systems for suppression of chemical and biological agents</p> <p>Segmented, reconfigurable, isolatable distribution fabrics for power, water, communications, and HVAC</p> <p>“Soft stop” technologies for intruders and other dangerous people.</p>
Secure, Distributed Collaborative Computing	<p>Approaches for creating trusted computing platforms</p> <p>Mechanisms that allow mutual exploration and negotiation of security policies</p> <p>Techniques for allowing mutually distrustful parties to share computing resources</p> <p>Network-oriented operating systems that allow for dynamic reservation of all types of systems resources, and</p> <p>Ways of ensuring that the digital “senses, nervous system, and brain” that make these things aware/smart cannot being used malevolently by an adversary.</p>
Effective Computer-Human Interaction	<p>Fielding sensor suites suitable for detailed observation of humans and developing techniques for extracting all of the available information about humans from their data streams</p> <p>Producing algorithms that not only identify individuals but characterize them with respect to a number of important features (especially as this relates to spotting “dangerous” people), and</p> <p>Creating systems that automatically develop cognitive models that allow them to adapt to individuals over time with a view to assisting these individuals with a variety of tasks.</p>
Privacy and Anonymity	<p>Develop system approaches that protect privacy within the system and</p> <p>Ensure that when personal information is conveyed outside the system, the person has full knowledge of who has accessed this information and for what purpose.</p>

<p>Sustainable Mechanisms for Recovery of Vital Services</p>	<p>For power:  Diagnostics for characterizing damaged energy infrastructure with plans for local repowering  Multifuel power sources (turbines/fuel cells) with appropriate power electronics, at all power levels, and  New ultra-efficient local loads (lighting, communication, sensing) to reduce demand.</p> <p>For communications:  The ability to rapidly deploy a cell system with acceptable linkages  Provide a supplemental communication system for response personnel  Develop system-linked specialized hardware for rescue, sensor net, and  Provide secure/verifiable wireless data links at all levels</p> <p>For water:  Providing mechanisms for water quality monitoring for pathogens, salinity, etc. In real-time  Making it possible to deliver potable quality from a wide range of sources, including closed and other non-conventional systems, and  Creating advanced waste-water treatment approaches that do not entail a massive physical infrastructure</p> <p>For healthcare:  Access to hospital level diagnostics and therapeutic mechanisms at incident site  Low manpower, just-in-time approaches for patient education, and  An intelligent system for ensuring efficient, coordinated response from all medical responders</p> <p>For security:  Develop systems that can automatically discriminate threats based on cameras, sensors and smart evaluation systems  Create “robotic”, self-teaching security systems to enhance local and area security through autonomous action  Produce mechanisms that allow these robotic systems to effectively team with human law enforcement staff, and  Field flow-control mechanisms that ease the job of monitoring/restricting movement of people in areas that have been attacked.</p>
--	--

## The Path Forward

In pursuing the development of these capabilities, we should work in two complementary directions.



In the first direction, the goal is to start with an “easy” problem and then expand the scope and complexity. In the case of structures, begin with the problem of creating a single, smart building, but then grow this to a smart campus and then to a smart city. In the second direction, the goal is to increase both the number of capabilities brought to bear and the degree to which these capabilities are integrated.

For example, the first smart building created may have a limited set of capabilities that each function intelligently yet independently. The HVAC system would be equipped with bio-threat detectors and independent heating/cooling zones such that detection of a contaminated zone could lead to immediate HVAC shut down in that zone and the adjustment of flows in other zones to minimize the spread of the agent. Likewise, the initial building design contains video surveillance and simple scene-understanding capabilities that allow the building to automatically assess the presence or absence of people in different areas of the building.

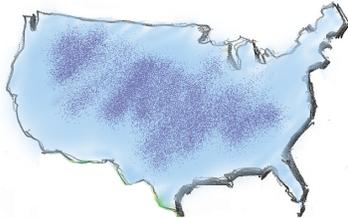
In later designs, a more capable scene-understanding algorithm could be added that allows the building to interpret activities viewed by its video cameras. In addition, a broader range of

instrumentation would be added to increase the building's perceptive abilities and data fusion software would be added that allowed the various sensor inputs to be combined into a common map of ground truth. As additional response capabilities are added (e.g., controls on building portals, chemical/biological agent suppression systems, or robotic vehicles for evacuation of victims), these and the sensory subsystems are all integrated with software that make the building capable of reasoned autonomous response. In the end, the goal will be to demonstrate the effective operation of these concepts in a large-scale collection of structures and other infrastructure elements, such as a city, in which the buildings, the utilities, the transit systems, etc., function as a whole to protect the city's inhabitants and to preserve the many missions that the city supports.

## SSB—SECURE AND SMART BORDERS

International commerce vital to the U.S. economy generates truly massive traffic across U.S. borders. The events of 9/11 underscore the importance of trying to achieve better control over that traffic, even while preserving the smooth flow of commerce.

### Border Management: The Flow of Legal and Illicit Goods and People



- In 1999, 475 million people, 125 million vehicles, 16.4 million trucks, and 5 million maritime 40-ft. containers entered the US
- Total annual US cocaine consumption can fit in 15 40-ft. containers
- 2.7 million undocumented immigrants enter US illegally each year
- 5-10 million pounds of CFCs smuggled into US each year

It is not clear that the increased inspections and delays have enhanced US security vis-à-vis the threat of terrorist attack.

US is more likely to suffer a WMD attack from terrorists using ship, trucks, or planes rather than from a foreign country using a long-range missile.  
— US Nat'l Intelligence Estimate (Source: Wash. Post, 1/11/02)

Secure and Smart Borders

2

To begin moving toward a “vision of the border of the future,” President Bush’s FY 2003 Budget proposes about \$11 billion for border security, an increase of \$2.3 billion over the FY 2002 budget. The Office of Homeland Security has laid out the requirements for the Smart Border of the Future (see box above). It should be a comprehensive system that eases legitimate trade while enhancing security against bad actors and contraband goods. The system should comprise a layered, but integrated, set of defenses, including:

- screening of goods and people before they reach U.S. territory,
- inspections of border traffic, and
- measures to ensure compliance with law after goods and people have entered the U.S.

Border control, law enforcement, and intelligence agencies should communicate seamlessly with one another. Pre-screening and certification of low risk traffic should permit closer attention to high-risk traffic. The system will require cooperative agreements with bordering states, major trading

### **The Smart Border of the Future**

“America requires a border management system that keeps pace with expanding trade while protecting the United States and its territories from the threats of terrorist attack, illegal immigration, illegal drugs, and other contraband. The border of the future must integrate actions abroad to screen goods and people prior to their arrival in sovereign U.S. territory, and inspections at the border and measures within the United States to ensure compliance with entry and import permits. Federal border control agencies must have seamless information-sharing systems that allow for coordinated communication among themselves, and also the broader law enforcement and intelligence gathering communities. This integrated system would provide timely enforcement of laws and regulations. Agreements with our neighbors, major trading partners, and private industry will allow extensive pre-screening of low-risk traffic, thereby allowing limited assets to focus attention on high-risk traffic. The use of advanced technology to track the movement of cargo and the entry and exit of individuals is essential to the task of managing the movement of hundreds of millions of individuals, conveyances, and vehicles.”

President George W. Bush,  
*Securing the Homeland,  
Strengthening the Nation*  
(Washington: The White House,  
February 2002)

partners, and private industry. An effective system will require advanced technology.

The Secure and Smart Borders BHAG takes its name from a declaration signed by the United States and Canada on December 12, 2001.<sup>3</sup> This declaration announces joint measures to try to establish between the two countries the kind of border system described above. Other U.S. Government initiatives are underway. The U.S. and Mexico will be discussing an agreement similar to that between the U.S. and Canada. The U.S. Customs Commissioner has described additional U.S. Customs Service measures aimed at achieving “smart” borders—with special emphasis on monitoring cargo container traffic.<sup>4</sup>

In sum, there is strong Federal interest in the notion of a comprehensive, multi-layered border control system. The analysis of the ACG team studying the border issue turned out to have closely paralleled Administration thinking. Not surprisingly, then, the team concluded that the government was on the right track. Nevertheless, the country has a long effort ahead before it actually achieves the “smart border of the future.” The Administration has recognized the need for advanced technology in realizing its vision, and we propose here lines of technology development in which Sandia could make major contributions.

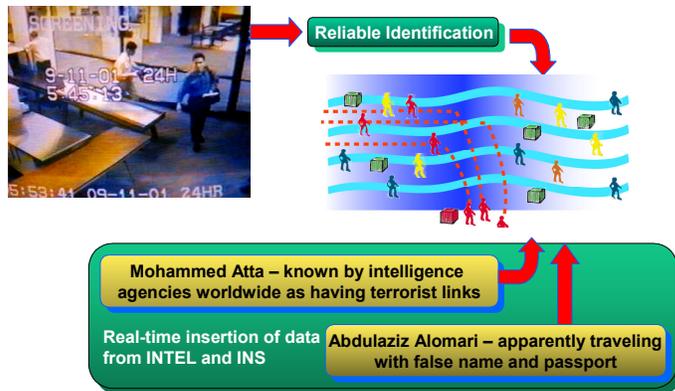
---

<sup>3</sup> See <http://www.whitehouse.gov/news/releases/2001/12/20011212-6.html>, accessed Feb 8, 2002.

<sup>4</sup> See <http://www.csis.org/goc/Bonner.PDF>, accessed Feb. 8, 2002.

## Example of Success

If only we had identified and tracked  
“bad actors” for cues...



It will never be possible to seal U.S. borders so tightly that potential terrorists will always be barred and the components of weapons of mass destruction will never enter. That is why the layered defense described in the introduction of this paper is necessary.

Nevertheless, it should be possible to raise the bar against bad actors and materials, significantly decreasing the probabilities of their penetration. For example, at least two of the 9/11 terrorists might have been stopped if border and airport security systems had been able to match them to intelligence, immigration, or law enforcement records. At a minimum, had they been accurately identified before boarding their flights, they might have been scrutinized more carefully as potential security risks.

## Technology Challenges

We describe here four lines of technology development that, especially if taken together, could significantly contribute to constructing the “smart border of the future.” The first line deals with all U.S. borders as a system; the other three pursue technologies that would solve particular problems in parts of the system.

First, the SSB program would design a **system architecture** that considered the multi-layered, multi-faceted border management problem as a whole. **This architecture would specify the appropriate roles for the other technologies pursued in the program.**

Second, the program would pursue the development of 3D optical radar for **facial recognition systems**, but also for a variety of applications at both border portals and perimeters.

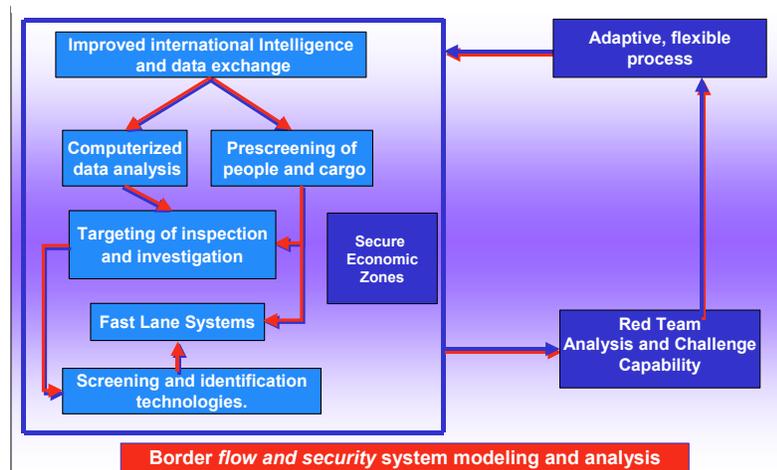
Third, it would develop a **“universal screening” portal** for monitoring and controlling the flow of people and goods through border entry points.

Fourth, it would develop an integrated set of techniques to **prevent the entry of weapons of mass destruction (WMD)** or WMD components into U.S. ports.

### *Global Border Flow and Security System Architecture*

People and goods flow into the territory of the U.S. through a complex system that extends well beyond either side of the physical perimeters and ports of entry that make up our geographical borders. This system offers many alternative routes for the penetration of bad actors and contraband. It also offers a variety of ways of screening and managing the flow. A detailed understanding of that system will require extensive research on, and modeling of, the system. Moreover, the system model will have to include an understanding of the interfaces and interaction of the system with other systems—particularly intelligence and law enforcement, both national and international.

## **Towards a Secure Border Architecture**



The "border" is a complex system

The program would begin, then, with the development of modeling and analysis tools for understanding the complex

nature of the border flow problem. The figure above illustrates some of the elements that would have to go into such a model. The central design principal is that technologies and procedures should contribute toward enhancing the flow of legitimate travelers and cargo so that greater scrutiny can be given to questionable traffic. The model should allow the testing and optimization of cost, performance, and vulnerabilities of existing and new technologies and procedures.

It is to be expected that as some smuggling paths become more difficult, bad actors will seek out other paths or will take countermeasures to the obstacles they face. To some extent, a system architecture with well-integrated internal sensors and communications will enable border management officers to adapt to the changing challenges posed by smugglers of people and goods. That is, they will be reasonably successful at playing the continuing game of counter-measures and counter-counter-countermeasures. For example, it may be realistic to keep the overall volume of drugs entering the U.S. down to some acceptable (even if still undesirable) level, even if it is not possible to reduce the level to zero.

There will, however, generally be a lag between the time that some number of smugglers have found holes in the system and the time that government can plug those holes. Because of the extremely high threat posed by terrorists, however, this kind of system learning may be insufficient—a few terrorists getting through and executing their plans can be, as 9/11 showed, a few too many. Therefore, it makes sense for the system to try to be preemptive as well as reactive. We propose, therefore, that a complete border system architecture, when installed, should include a continuous “red team” analysis and challenge capability. This capability should include personnel who are dedicated full-time to looking for ways to penetrate the system, and those personnel should be able to use the system model both to probe for vulnerabilities and to test methods of attack. They should also have access to law enforcement and intelligence information that might suggest more likely sources and means of penetration. Moreover, the red team challenge capability should include not just virtual probes in the simulated system, but real, operational exercises against the actual system. The results of this continuous red teaming should then be fed regularly back into the system in the form of responsive changes in technologies and procedures. Thus, the red team becomes the surrogate for smugglers and terrorists, allowing the system to learn and adapt even while the genuine threats remain latent, infrequent, or undetected.

Not only would the proposed modeling and analysis tools be used to test technologies and procedures for detecting bad actors and contraband, but they would also help assess measures for improving the flow of legitimate traffic. For example, one measure that could be evaluated is the secure economic zone. Such a zone between the U.S. and Mexico could reduce the traffic that has to be monitored by locating many of the objectives of cross-border travel—such as shopping malls, entertainment, factories, or warehouses—within zones straddling the border. U.S. travelers and goods would enter and exit the zones only through the U.S. side, while Mexican travelers and goods would enter and exit only from theirs. Thus the amount of inspection and identification needed would be very small even as the economic benefits of the traffic were maintained.

The system-architectural work for the secure economic zone concept would have to include at least the following elements:

- determination of the prospective percentage decrease in the need to screen and inspect people, cars, and trucks;
- cost-benefit analysis of the zones compared to alternative measures;
- study of legal issues and precedents for establishing binational economic zones.
- detailed zone designs (e.g. included facilities such as shopping malls, factories, entertainment, and restaurant; entry and exit monitoring systems; internal security)
- identification of necessary partnerships among businesses, developers, US-MX government agencies; and
- determination of appropriate sites for testing the concept.

Many agencies have interest and responsibilities in border security management. At this time it is not clear how reorganization to manage homeland security in the future. The primary U.S. border management agencies today are the Immigration and Naturalization Service (or INS, under the Department of Justice) and the U.S. Customs Service (under the Department of the Treasury).

Many other government agencies have responsibilities for one aspect or another of border management. For example, the State Department decides whether to issue visas to foreign visitors. The Coast Guard patrols the sea borders. Along with Customs, various other agencies of the Treasury Department, as well the FBI, attempt to track and intercept financial assets of terrorist groups and others. The Drug Enforcement Administration works with Customs to interdict drug smuggling. The Food and Drug Administration works with them to bar entry of unsafe food

imports. Obviously the intelligence community and the border management community must frequently share information and cooperate.

Because the FAA regulates U.S. international airports and carriers, and because domestic flights are vulnerable to international terrorism, the FAA also has a stake in the border management architecture. Private sector stakeholders include airlines, trucking companies, railroads, ports, shipping lines, customs brokers, freight forwarders, manufacturers, and receiving firms. Finally, foreign counterparts to the U.S. stakeholders have interests in their nation's commerce integrating well with U.S. border management systems. That integration may include the deployment of standardized technology and procedures abroad as well as in the U.S.—particularly for pre-screening U.S.-bound people and cargo.

The fundamental systems analysis and computing capabilities that would be required to design a comprehensive border management architecture already exist in many places. The architecture does not exist now both because of the common problem of multiple, diverse government agency responsibilities and budgets, and a lack of urgency before 9/11 that now appears to have changed. The border management agencies of government are beginning to try to better coordinate their plethora of databases and functions, but there is a long way to go.

Some pieces of the architecture problem have already been started. For example, with DOE-NNSA funding, Los Alamos National Laboratory has begun a Maritime System Study to develop models to assess the value of alternative surveillance technologies and strategies for interdicting illicit shipments of WMD materials. A technical working group supporting this effort comprises representatives of NNSA, LANL, the Office of Naval Intelligence, and the Coast Guard (under the Department of Transportation).

Sandia researchers have previously conducted systems analysis relating to the U.S. border with Mexico. One study focused on reducing illicit traffic across the perimeters, or sectors of the border between legal crossing points.<sup>5</sup> Another focused on

---

<sup>5</sup> Advanced Systems Integration Department 9561, *Systematic Analysis of the Southwest Border* (OUO) (Albuquerque, NM: Sandia National Laboratories, January 1993).

control of container traffic through legal ports of entry.<sup>6</sup> The team conducting the latter study subsequently proposed an “Advanced Cargo Surveillance System.” Sandia also operates the National Institute of Justice Border Research and Technology Center in San Diego. Further discussion of architectural issues for monitoring cargo flows is found below in the section on Advanced Cargo Surveillance.

### *Facial Recognition Technology*

The recent U.S.-Canadian “Smart Borders” initiative includes a provision for a biometric identification card for frequent border crossers, as does the U.S.-Mexico Border Crossing Card. This is one example of how an accurate and reliable identification system can improve border security while also smoothing the flow of legitimate traffic. Extending the concept beyond frequent crossers to all alien visitors could further enhance security.

All visas issued to visit the United States could take the physical form of a biometric ID. Once the initial visa was issued, the U.S. would have a record of all future entries and exits of the person through U.S. border-crossing facilities. If the ID system were standardized to other countries, these countries and the U.S. could share travel histories of individuals with each other, possibly cuing further investigation of suspect patterns. Once a person had received such a visa, it would be impossible (if the ID system were accurate enough) for that person to leave or reenter the country using a different name or identity. Again, if other countries used compatible means of identification, false passports or other national identity documents would also be more difficult to obtain and use.

A possible alternative to the issuance of biometric visa-IDs might be extremely accurate and reliable facial recognition technology. Such technology would permit the construction of a database of the faces all those entering the .S. at border-crossing facilities. (Or, before entry, visas could require sufficient photographic data for the database, and the face of person attempting to enter could also be matched against the person getting the visa.) Faces of people applying for visas or attempting to enter the U.S. could be matched against those in any watch lists containing photos, providing some improvement to current watch-list checking.

---

<sup>6</sup> J.B. Godfrey et.al., *Advanced Technologies for International and Intermodal Ports of Entry (ATIPE)* (Unpublished, September 1997).

With adequate technology, persons having legally entered the U.S. might later be covertly identified in airports or any other places where monitoring faces was feasible. Again, this capability could help with INS, law enforcement, or intelligence investigations or surveillance. The system could also verify that those entering the country legally were leaving within the period allowed by their visas, thus helping to keep current the database of those who had not left and should be investigated. If the ID were required for further use once the visitor had entered the U.S., it would be of potential use of INS, law enforcement, and intelligence investigations. For example, if it were required for situations in which U.S. citizens must provide a social security number—e.g. getting a driver’s license, establishing bank or credit accounts—it would provide a means of tracking some activities. If comparably accurate IDs were established for U.S. citizens, the ability to detect anomalous behavior by visitors would be greatly enhanced.<sup>7</sup> Note, however, that there is already opposition to this strategy by groups concerned about threats to civil liberties.

*Universal Screening Portal – A Systems Approach to Efficient Screening of People and their Possessions*

The objective of a Universal Modular Portal is to provide a comprehensive screening system that could be used at most any point in a “border” system. Future borders must be viewed as a system of corridors, starting at the point of origin and extending

---

<sup>7</sup> Because the most frequently used ID document is the driver’s license, the American Association of Motor Vehicle Administrators has proposed the following set of measures for the US and Canada:

1. Improve and standardize initial driver’s license and ID card processes.
2. Standardize the definition of residency in all states and provinces.
3. Establish uniform procedures for serving noncitizens.
4. Implement processes to produce a uniform, secure, and interoperable driver’s license/ID card to uniquely identify an individual.
5. Establish methods for the prevention and detection of fraud and for auditing of the driver’s license/ID processes.
6. Ensure greater enforcement priority and enhanced penalties for credential fraud.
7. Seek U.S. federal and other national requirements for legislation, rule making and funding in support of AAMVA’s identification and security strategies.

(<http://www.aamva.org/drivers/drvIDSecurityExecutiveSummary.asp>).

to checkpoints, hubs, and perimeters at all levels. It is even necessary to consider concentric series of checks at “internal borders” within the U.S. To advance the vision of smart and secure borders, this universal portal needs to:

- reduce the number of unknown contraband and people crossing borders;
- enhance the flow of commercial cargo and people; and
- enable subsequent tracking of potential threats by integrating monitoring with intelligence and law enforcement information.

In moving toward a modular portal architecture two concepts should be pursued: 1) increasing levels of system integration and 2) expanding borders to zones. Since one of the objectives for a smart border system is flexible adaptability, this modular architecture should permit the integration of new capabilities over time to counter a dynamic threat environment. A modular system solution will allow for integration of multiple technologies to achieve within 5 years the screening goals of a) reliable identification of people using non-intrusive surveillance and b) multi-modal contraband detection.

For the longer term of 5-7 years, the portal architecture should adaptively incorporate additional detection capabilities. It may also be possible to develop prototype systems that will reliably recognize individuals. More ambitiously, perhaps it might become possible to identify the *intent* of an individual. This is by far the most controversial technique proposed in this report. Screening people based on technology-based measures of their intent will evoke major concerns about privacy issues and constitutional rights. Nevertheless, research suggests that there are subtle indicators that humans unconsciously recognize as threatening. If technical measurements of these indicators can be taken, they might form the basis for a good first filter for checkpoint screening, after which additional screening measures could be applied. Given the potentially catastrophic consequences of terrorist acts, the possibility of an “intent screen” should at least be explored. When, whether, and how the technology should be deployed, however, will also require extensive examination from legal and political points of view.

The applications for a universal portal screening system include, but are not limited to, airport terminals, high profile events, and sensitive facilities, embassies, border checkpoints. For high security areas, such as nuclear materials handling areas, personnel are already screened to check individual authorization

and to prevent nuclear material theft or sabotage. Such checkpoints would also benefit from advanced architectures and technologies for automating, integrating, and improving the screening process.

### **Personnel Screening**

In current security systems, the screening of personnel entering a controlled access area is based on access authorization and identity verification. Typically this screening uses 1) something you have; 2) something you know; or 3) something you are, i.e. biometric verification. Biometric identification is based on the measurement of a physiological and/or behavioral characteristic of an individual. Biometrics, then, can be defined as the science of using a particular biological aspect of the human body to recognize and verify a person's identity. They include fingerprints, retinal or iris scanning, hand geometry, voice patterns, facial recognition, and other techniques. Automated biometric identification got its start in the late 1970s and grew slowly until the late 1980s or early 1990s. Initially, biometrics were employed primarily in special high security applications; today, the technologies have developed far enough to be considered for many more applications.

One possible antiterrorist application would be surveillance with biometrics to autonomously and continuously screen large numbers of people at border crossings. Automated access control for prescreened travelers would allow such travelers to pass quickly through the portal, permitting allocation of resources to closer scrutiny of others. The pre-authorized individual could be quickly matched one-to-one with his or her record in pre-enrolled template. Those not enrolled in the system could be subjected to more intensive security screening. This screening might include comparison to those in a database of known or suspected criminals or terrorists. For this purpose, the most effective biometric may be facial recognition (see section above on optical radar), since other biometric measurements than a photo may not be available for many individuals of concern.

The ability to monitor characteristics of people or recognize features that indicate malevolent intent is of interest in all screening checkpoint applications. In fact, current U.S. INS and Customs inspectors have developed intuitive abilities to home in on suspicious individuals. Some research indicates that expressions, changing heat levels around the eyes, blushing patterns, or pupillary response may indicate deceptive or

malevolent intent. It is desirable to understand the knowledge and intuition being applied by current inspectors, then to investigate whether automated techniques and systems could assist in them in their screening functions.

### **Contraband Screening**

Existing portal screening products (metal detectors, special nuclear material detectors, swipe analysis with chemical detectors, x-ray systems, ID verification) provide checks in a standalone fashion, not an integrated system. We propose consideration of new techniques that integrate multiple, complementary technologies that are employed in a variable, unpredictable constellation of screening measures. An automated checkpoint with multi-modal contraband detection capability could provide several advantages. First, it is possible to combine two or more technologies that complement the weaknesses of the other. Second, automation could remove the security screeners from direct contact with potential adversaries during initial screening, thus minimizing and the possibility of injury or death to members of the security force. Third, utilizing multiple technologies in a flexible and adaptive screening process could reduce the predictability, and therefore the vulnerability to evasion, of the security measures in place.

### ***Advanced Cargo Surveillance***

According to a recent National Intelligence Estimate, “the U.S. is more likely to suffer a WMD attack from terrorists using ship, trucks, or planes rather than from a foreign country using a long-range missile.”<sup>8</sup> The solution to this problem will require development of an integrated set of defensive techniques. Effective cargo surveillance demands a layered approach that includes pre- screening, certification, targeting, and inspections.

Advanced sensing capabilities—possibly linked to response, delay, denial, and neutralization systems by distributed secure information transfer systems—have the potential to enhance cargo transportation efficiency and security. A strategy worth exploring for feasibility, cost, and effectiveness is to equip shipping containers with sensor systems to monitor internal conditions. Such sensors installed on sealed and tagged containers could assure the continuing absence of indicators of contraband. Customs officials could quickly pass over certifiably

---

<sup>8</sup> Reported in *Washington Post*, January 11, 2002.

clean cargo in the smart containers, concentrating inspection efforts on less trusted containers.

Smart container concepts with integrated sensor systems are not new, but the necessary low cost, low power, sensor packages have yet to be developed. Advanced low cost sensor techniques and systems could also add speed and security to customs screening and inspection of questionable containers.

Stakeholders from both the public and private sectors are interested in enhancing the flow of cargo and goods while preventing the smuggling of contraband materials. The government must be mindful not only of security, but of the economic harm that can come from serious impediments to the smooth flow of legitimate imports and exports. Industry will resist security solutions that impose heavy costs and delays.

### *Smart Container Concept*

A smart container program would explore means of speeding the flow of benign cargo containers while permitting greater attention to be devoted to higher-risk containers. It would examine combinations of sensors embedded in containers as well as external sensing systems, tags and seals, and tracking and communications systems.

There are already numerous independent technologies for the detection of the presence of contraband in containers and trucks at border crossings. There has been limited development and commercialization of systems to monitor the contents of a container for the presence of contraband on a continuing or on-demand basis. Sandia developed the Advanced Cargo Surveillance Information System (ACSIS) between 1994 and 1997 to address the problem of concurrently increasing security measures and moving more freight faster, cheaper, and with higher reliability. ACSIS addressed the problem of speeding the physical flow of goods by improving information flows on documentation of shipments. A key concept in ACSIS involved moving the documentation processes away from the borders so that information was available and analyzed before the cargo even reached the border. For example, cargo approaching an international border or zone would electronically file its documentation in advance to allow for clearance prior to arrival. Pre-cleared ACSIS subscribers could then move quickly through express service lanes.

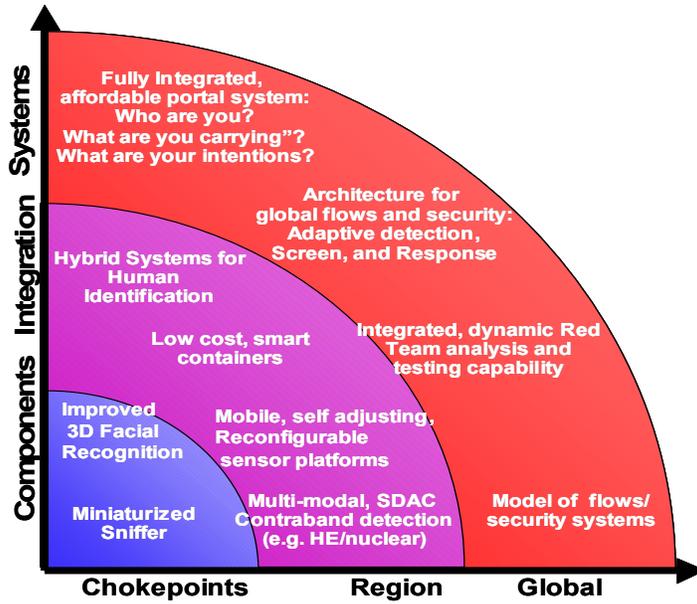
Another key concept in ACSIS was to link several types of cargo information, such as current location, status, and documentation. Today some transportation entities track their shipments with GPS transponders to ensure on time delivery for just-in-time manufacturing lines. Commercial systems now available can also track cargo documentation (point of origin, points of transshipment, origin of goods, etc). At least some international companies are motivated to implement transparent systems for tracking cargo to reduce delays and costly inspections at ports of entry.

Today, customs inspectors have to pay more attention to detecting biological and chemical substances (explosives, anthrax, narcotics). There are developments underway on “sniffer” systems that circulate air through pre-concentrators to detect minute amounts of target substances. An advanced concept for an adaptive sensor system is a programmable, integrated biological/chemical /radiological detector system that could receive instructions from authenticated parties to detect a substance of particular interest and set thresholds.

Once sensors are in place, there must be some mechanism for communicating the sensed information to only those who need to know. In a border application, if Customs were to identify something suspicious (or poorly documented) about a shipment, they might be able to communicate with others involved in the shipment process to resolve the issue before the freight reached the border. These same technologies can be used to get quick response (police, EMS, etc.) in case of a crisis with the shipment or the carrier. There is already a commercial system like this for HAZMAT so that first-responders know what kind of situations they can expect (it is more of a database lookup, though, as opposed supplying to real-time information). For the smart container concept, the communication equipment may need to be integral to the container itself, and the sensor system would probably have to be add 10% or less to the cost of the container.

## The Path Forward

The figure below captures the concepts for moving forward with improved smart secure borders.



## FACETS—FRACTAL APPROACHES FOR CLARIFYING AND ENABLING TIMELY SUPPORT

An analysis of the timeline of events that occurred on September 11 shows clearly that we lost first responder lives in the WTC because situational understanding was slow. This loss is common when people are forced to deal with first-of-a-kind, dynamic, information-sparse situations. With meager information (except for that gleaned from personal observation) and with few external resources readily available, decision makers at the scene of a crisis are handicapped and lives are often lost. There are 43 agencies involved in Homeland Security, but on September 11, citizens with cell phones made the difference in providing an informational network. This BHAG is about finding a way to make situational understanding more seamless, more agile, and more timely.

FACETS aims to provide a powerful, fractal-based approach to design that would supply multi-user, need-tailored tools for rapidly understanding intrinsically foggy situations. This would include attack detection, attack assessment, defense assessment, decision guidance, and response. The fractal nature hinges on the themes of Sense, Decide, Act, and Communicate that recur throughout the threat detection and response system. The system would be dynamic, adaptable, and federated, with the focal point changing as the needs of its numerous members change. The system would have two operating modes:

- a pre-and trans-event mode that would monitor and expose developing situations to allow interdiction, and
- a post-event detect and analyze mode to enable optimal response.

The fractal approach calls for a common set of inputs, outputs, and value-added processes to occur repeatedly throughout the nation's response system. The design and development of a common architecture would allow these elements to be integrated easily into a dynamic, adaptive system that would raise the probability of terrorist event detection and dramatically improve the ability of the nation to respond to catastrophic events, both natural and human-initiated. This system must utilize both "push" and "pull" technologies, with the ability to pull information from sensors and databases, the ability to push information through the communication channel, and the ability to receive pushed information. Another key feature of this design would be a set of training simulators that could be easily

configured to simulate a wide variety of crisis situations, allowing for realistic training and evaluation sessions.

A fractal is defined as a self-similar pattern repeated at ever-smaller scales to produce irregular structures. For a geometric object, any suitably chosen part is similar in shape to a given larger or smaller part when magnified or reduced to the same size. In the context of system architecture, “fractal” implies that the collection of operating units is not necessarily predefined or hierarchical and that any unit of the structure is similar to any larger or smaller unit in basic function and communication standards. The advantage of a fractal design philosophy is that it contains common elements and interfaces that scale easily, have self-identifying attributes, and can reorganize as needs dictate. These repeating elements would be applied at all levels. For example, fractal units could be developed for:

- military operations
- law enforcement
- intelligence
- public health
- first responders
- scene commanders
- government
- the involved citizen (e.g., office manager)
- buildings
- building entries
- sensor systems

An architecture for such a system will need to define interface specifications, some common required elements and capabilities, message and event passing/handling /management, and required triggers. The fractal units which comprise the system will need to be autonomous but connected, so they can self-organize dynamically as the situation evolves. Thus communication and data-sharing channels would be optimized “on the fly” to get the right information to the right person in a timely manner. The system would have a normal background mode to collect and flag anomalies for characterization and possible interdiction, but would immediately switch to a support mode during a significant event.

The fractal approach of FACETS is based on a design utilizing basic units with four key functions integrated by a “manage” function. Specifically these functions are the ability to:

- **Sense** utilizing input from sensors, databases and people,

- **Decide** utilizing decision support tools and predictive, real-time modeling to provide the ability to process all relevant information,
- **Act** through a rich toolset to implement appropriate actions with appropriate command and control features. This implies the ability to know what resources are available and relevant.
- **Communicate** including the ability to receive critical communications and to automatically send critical communications.

The system must be integrated by a Manage node, which usually includes human as well as mechanistic elements. The Manage node function involves decisions about when to act, proper data storage and retrieval capabilities with the ability to query other data sources other data sources through the communication channel.

A FACETS system would have an architecture that would be fractal in its nature. That is, it would incorporate self-similar elements through defined input/output specifications, communication protocols and some key common elements. These would allow for “plug and play” operation and easy integration of information. The goal of this design would be to generate appropriate situational understanding - awareness plus decision support - including visualization and communication.

Each fractal element would be autonomous but connected, with decision-making decentralized but federated. Because of the fractal approach, elements would be able to self-organize dynamically as the situation evolves. This will allow communication and data-sharing channels to be optimized on the fly through distributed decision making to get the right information to the right person when needed. This also allows the system “focal” point to change as the situation changes; with elements moving from a central action role to a support role or vice versa. The access protocols would enable rapid, need-gated sharing of relevant information and system tools would assist the dynamic creation of command and control protocols.

The system would have a normal background role in monitoring and interdiction; with the ability to shift to a response and assist mode during critical events. A key feature of this monitoring mode would be the ability to collect and mine “anomalous” events from infrastructure monitoring as they occur, combine these with intelligence data, and thus

increase the probability that terrorist scenarios can be identified and stopped. System analysis capabilities would be able to assist during both natural and human-initiated events. The system would also be able to supply predictive modeling in real time to the scene and it would include responder tools such as education, virtual experts, and artificial experts.

Response elements would be system-optimized through the use of many small, inexpensive fractal SDACs throughout the system for initial detection. More sophisticated fractal SDACs on key elements, such as first responder units, would be used to add detail. In fact, a suite of fractal SDACs for specific missions of critical interest or need (e.g., all-border crossings, state of health, city-state) is envisioned.

The benefits of adopting this architectural approach are many. This fractal architecture would allow for a dynamic, adaptive system for easy growth of the system adjustment to loss of elements during operation. Since the system would NOT be hierarchical by design, it would continue to function even if connections were severed. It would distribute networked information to reduce vulnerability to loss of critical nodes. It would seamlessly create “virtual” communication channels and distribute critical information as required. It would use ubiquitous sensors to collect information, intelligent computer algorithms to find it, and advanced visualization technologies to present it in ways that assists human decision-making. It would integrate all sensor, intelligence, and database information into a common, whole-system view of events as they unfold.

The operation of the system would change as the need changes. Depending on which “unit” observed, different information and capabilities would appear, although the basic underlying design and interface would be as self similar as possible to make integration of different components as simple as possible and change of users as simple as possible. The system could enable access (through a broker service) to advanced decision support and modeling tools to help answer “what-if” questions at the scene. For example, if the question were, “If this chlorine tanks fails, what area should I evacuate?” the system would enter real time meteorological data into atmospheric dispersion codes to produce decision guidance. Finally, the system could assist end-users in crisis prevention, preparation, and response by providing predictive and real-time situational analysis.

Being fractal, the system could become operational with a few nodes, but then expand. The system should be vendor and

technology-independent; since it only requires that standard interfaces and common elements be implemented in a “plug and play” manner. This standardization could be supplied to existing systems with a “wrapper” or shell. Note that this is NOT a command and control system. It would interface with command and control systems, but here the intent is to process and feed information to nodes, not require all information to pass to a central node to be redistributed.

### **An Example Of The Benefits Of A FACETS System**

The following is an example of how an operational FACETS system could have responded to the events of September 11. The scenario assumes nodes for the FAA, Law Enforcement (FBI), Intelligence, an infrastructure analysis site (for structural analysis), New York City government, the NYC fire and rescue units and scene commander, the World Trade Center building, and citizens (workers) within the WTC. The initial actions would have been taken when the law enforcement node received anomalous data (a plane is not responding to radio) matched in real time with other events related to planes and terrorism (report of student suspected as a possible terrorist). For this reason, this example starts with events that occurred about a year before the WTC attack. While it is unlikely that the system could have created a full enough picture soon enough to shoot down the first plane, it could have certainly prepared decision makers for the subsequent events over the next hour and a half. After the first plane struck the WTC, the system would have gone to a response mode, assisting the first responders and the city with additional information to help them deal with the crisis.

## Comparison of September 11 Events, Response, and a Proposed FACETS Response

Time <sup>9</sup>	What happened	What we did	We could have done
Fall 2000	Suspected terrorist Jarrah enters U.S.	Let him in and failed to track	Marked him as suspicious and tracked his movements
Jan 2001	Atta questioned on violation of visa and taking flight lessons	Let him enter; extended tourist visa	Marked him as suspicious and tracked his movements
Aug 2001	Moussaoui jailed in Minn. After requesting 747 flight simulator training	Flight school alerts FBI that 747 could be used as a “bomb”; data goes ????	Enter report into system for future mining
7:59 AM	AA#11 departs Boston		
8:01 AM	UA#93 from Newark leaves gate but is delayed on the ground		
~8:10 AM	AA#11 turns off transponder and quits responding to radio	Nothing	Enter “anomalous” entry into system and tracked
8:14 AM	AA#175 takes off from Boston	Nothing	
8:20 AM	AA#77 takes off from Dulles	Nothing	
8:24 AM	UA#175 reported hearing suspicious transmission over open mike	Nothing	Enter report and tag to AA#11 report; hijacking is suspected; inform NORAD; tie hijacking to Moussaoui report and existing statements; suspect use of plane as bomb; pass to NYC that planes are headed their way
8:40 AM	FAA notifies NORAD that AA#11 has been hijacked	Nothing	Scrambled fighters
8:42 AM	Flight UA#93 takes off from Newark	Let it take off	Kept all planes on the ground pending resolution of suspected hijacking
8:43 AM	FAA notifies NORAD that #175 has been hijacked	Nothing	
8:45 AM	AA#11 crashes into North tower of WTC	Called 911; started evacuation of North tower; started, then apparently tried to stop, evacuation of South tower	Create tie to NYC scene command; report second plane on the way; NYC starts evacuation of other tall buildings in city
8:46 AM		Military sends fighters (toward NYC?) from Falmouth, Mass	Tie NYC to building expert system to analyze damage
9:02 AM	#175 crashes into South tower	Responded by sending rescue into buildings	South Tower now empty; collapse of building predicted by analysis
9:21 AM		NY Port authority orders all bridges and tunnels in NY closed	Provide information on infrastructure damage and evacuation routes
9:24 AM	FAA notifies NORAD that #77 was hijacked		Fighters intercept #77
9:35 AM	Approximate time #93 was hijacked	NORAD sends two fighters from Langley	This plane is still on the ground
9:38 AM	#77 crashes into Pentagon	Called 911	
9:40 AM		FAA halts all flights in US	
9:45 AM		White House evacuated; passenger from #93 reports hijacking and their attempt to regain control	System helps coordinate evacuation of critical areas
9:57 AM		President Bush departs Florida toward secure location	
10:05 AM	South WTC tower collapses	Tried to get rescue workers out of North building but had trouble with communications	No one in South tower; multiple communication channels help warn emergency personnel of danger of collapse
10:08 AM		Secret service with weapons deploy across from White House	

<sup>9</sup> All times in the scenario in are Eastern Daylight Savings on Sept. 11.

10:10 AM	#93 crashes in Penn. Countryside; portion of Pentagon collapses		This plane is still on the ground
10:13 AM		UN evacuates	Should have been done an hour earlier
10:24 AM		All inbound transatlantic aircraft diverted to Canada	Should have been done an hour earlier
10:28 AM	WTC north tower collapses		
10:45 AM		All federal buildings in Washington are evacuated	
~11:00 AM		Kirtland Air Force Base elevates alert level; Sandians told to evacuate	Should have happened much earlier
12:04 AM		Los Angeles airport evacuated	Should have happened much earlier
12:15 PM		San Francisco airport evacuated	Should have happened much earlier
12:30 PM	FAA reporting 50 flights in U.S. airspace; none reporting problems		
1:44 PM		Pentagon dispatches five warships and two carriers to protect the East Coast	Should have happened much earlier
4:10 PM	Building 7 of WTC on fire		
5:20 PM	Building 7 collapses		
6:45 PM		President Bush arrives back at White House	
8:30 PM		President Bush addresses nation from White House	

## Technology Challenges

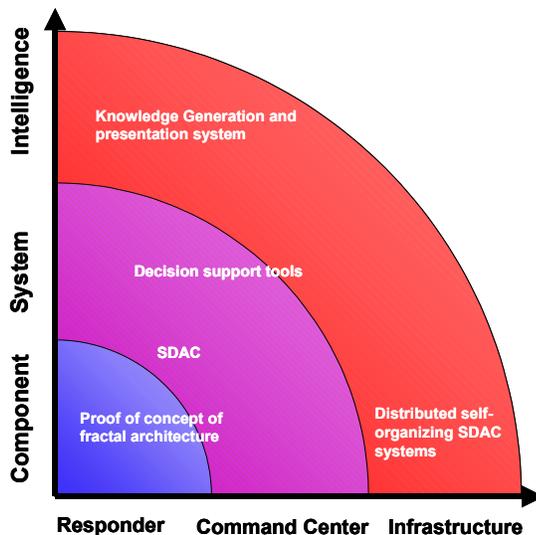
Once we have defined the appropriate critical elements, the architecture for Fractal Sense/Decide/Act/Communicate systems should be structured to enable collective behavior and allow easy integration into larger systems.

We believe this architecture has not been previously considered. Most emergency response tools tend to be hierarchical, with information often guarded by a “gatekeeper” at each level. The flow of information is intrinsically slow in many crisis events. During the events of September 11, as detailed in the previous section, the slow flow of information to the appropriate officials precluded an accurate assessment of the situation.

There are many aspects of this architecture that need to be explored. First we need to know what realizable fractal architecture would look like. This might encompass the design of organizational structures, the design of communication systems, the design of software or hardware for computing or for the architecture of distributed computing operating systems. Then we need to know whether or not these architectures are really different than current approaches and if so, what real benefits there might be.

## The Path Forward

The figure below outlines the roadmap for developing FACETS. Central to FACETS is the development of a fractal architecture. Once this foundation has been defined, the primary components can then be developed and integrated. The SDACs represent the autonomous fractal units (nodes) of the system. Working



together and self-organizing, the SDACs perform functions exceeding the capability of a single unit. Knowledge generation from a network of SDACs will be an important natural product. The human/machine interface is a critical element at this phase and advanced visualization methods need to be developed to effectively present the system knowledge. Together with the decision support tools, FACETS will provide exquisite situational awareness to aid decision makers during future terrorist attacks or other disasters at each level of command: local, state, and national.

## DICTUM—DYNAMIC, INTEGRATED CAPABILITY FOR THREAT UNDERSTANDING AND MANAGEMENT

The al Qaeda Leadership and the Pentagon apparently agree on one major point: understanding of the enemy—intentions as well as capabilities—is essential for victory. U.S. and foreign intelligence organizations have for many years used traditional intelligence methods (such as collecting information, monitoring movements, and analyzing capabilities) to successfully interdict terrorist operations. But these methods proved insufficient to prevent several large-scale attacks (Aum Shinrikyo, Oklahoma City, Kobar Towers, World Trade Center 1993, U.S.S. Cole, World Trade Center 2001, and others) that led to loss of thousands of lives and of billions of dollars. In retrospect, it appears that information that could have alerted us to the attacks was in our possession, yet we failed to synthesize the facts and recognize their significance. Moreover, the level of damage and frequency of attacks have increased as we seriously underestimated the capabilities, operational sophistication and planning, and degree of violence that terrorists were willing to use.

September 11 showed that we lack effective means for understanding our enemies and their intentions in order to recognize, anticipate, and deter their behavior. For the War on Terrorism to be successful in the long term, and to return a sense of safety and security to the nation and to the world, we must develop new approaches and tools. We must examine what has limited our ability to respond effectively to the escalating occurrences of terrorism. Effective responses might range from demotivation at the root cause level, to dissuasion at the embryonic stage of terrorist activity, to deterrence at the active growth stage, to disablement at the fully developed stage of terrorist cells or groups.

We assert that this understanding is greatly hampered by the lack of:

- consistent and systematic analysis of available information that exists;
- tools to integrate multidisciplinary bodies of knowledge and transform them into integrated models that adequately characterize complex terrorist networks and the behavior dynamics within them,
- dynamic, adaptive tools to simulate and explore the complex systems of terrorist groups;

### **Know Thine Enemy**

"Information about the enemy's intention provides early warning signs for the command, which in turn makes appropriate preparation and thwarts the enemy's opportunity"

*Al Qaeda Training Manual, 1998*

"Exquisite" intelligence on the intentions and capabilities of adversaries can permit timely adjustments to the force and improve the precision with which it can strike and defend."

Donald Rumsfeld, *U.S. Nuclear Posture Review*, January 3, 2002

"The nation that wants to achieve victory over its enemy must know that enemy very well. It also must know the site of the battle in detail. Those who fight an enemy that they do not know do not win because a successful military plan must be built on clear and trustworthy information. The commander who fights an enemy and does not know his strength is blind and destined to fail and fall."

*Al Qaeda Training Manual, 1998*

- means to reduce perception bias in analysts developing, simulating and exploring representations of such complex systems.

It is clear that we cannot consistently “see” and “discriminate” data and information indicative of anomalous behaviors (or activities that have a high-risk potential), high-risk individuals, and rapidly evolving, adaptive threats

We propose developing capabilities to:

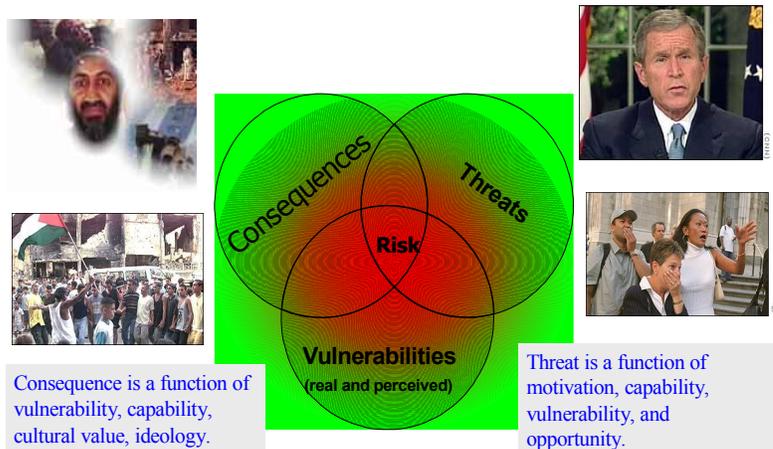
- build, link, and effectively explore and exploit data and knowledge bases of terrorist behaviors, drawing information from multiple disciplines (engineering and physics, behavioral sciences, cognitive sciences, intelligence and law enforcement, military, etc.) which, when integrated, might provide us with a clearer picture of the complex system of terrorist-target behaviors;
- systematically analyze and test what we know about terrorist behaviors;
- build dynamic, adaptive, tools for modeling and simulating these integrated, complex systems through "what if" simulations and "war-gaming" exercises; and
- explore the effect of multiple, differing perspectives and perceptions of the same reality when considering our decisions about terrorists and their behaviors, and when anticipating terrorist responses to our actions.

By developing such capabilities, the community could make significant contributions towards the “exquisite intelligence” called for by Rumsfeld. For example, these capabilities would enable intelligence community, military, law enforcement, and policy arms of the U.S. government to accurately see, and perhaps learn and anticipate, patterns and indicators of terrorist behavior. These efforts would drive improvements in technical development of data mining, sensors, monitoring systems, and tools for military or intelligence responses to terrorist activities. The assessment and policy communities could explore multiple options and their potential outcomes in complex decision spaces, gaining insight into potential unintended consequences of decisions. On the basis of such information, our government leaders could more effectively devise a balanced, appropriate portfolio of technologies and policies for demotivation, dissuasion, deterrence and disablement of terrorists.

A current approach for analyzing terrorist activities and the potential for attack relies on a risk framework that considers threat, consequence, and vulnerability. In this framework it is readily recognized that threat is a function of motivation,

capability, and opportunity. However, this risk framework has focused on the analysis of capability, the assessment of vulnerabilities and what to do about them, and the engineering analysis of potential consequences. This approach has been found wanting, as we saw on 9/11, because it

- ignores the terrorists' potential for innovation,
- fosters erroneous assumptions that divert attention from potential vulnerabilities, and
- ignores the differing assessments of consequence that terrorists may be making, thus leading to misestimates of the "real" risk.



### Risk Evaluation Requires Multiple Perspectives on Interdependent Variables

Intelligence analysts, law enforcement and security personnel, and policy-decision makers were hampered prior to 9/11 not only by a deficient framework for assessing risk, but by approaches to data analysis that failed to detect indicators of terrorist attack. Many have suggested the need for advanced data mining, exploration, and exploitation to better pick up signals in high noise situations. But how are we going to be able to tell data mining programs what signals to look for? How are we going to understand the adaptive nature of terrorist behavior patterns in order to know what new patterns to look for? Without such understanding, our data exploitation capabilities are still at risk of failing to alert us to the next attack.

Intelligence efforts have focused mostly on ascertaining the technical capabilities and movements of known, sophisticated sub-national threats and terrorist groups. In addition, however, there is a body of knowledge based on psychological studies of the high-level goals, motives, and ideology of known individual

and groups of terrorists. Between these "soft" studies and the "harder" studies of technical capabilities and movements, there is a chasm. No bridge brings the two bodies of knowledge together to form an understanding of how the doctrines, rationales, assumptions about the world, and values of terrorists influence their organization, operational procedures, and innovation.

We propose the development of a Dynamic Integrated Capability for Threat Understanding and Management (DICTUM) to bridge this gap between intelligence and the new threat environment. The goals for DICTUM are to:

- build new analytical capabilities to understand terrorist behaviors through multi-disciplinary conceptual models of terrorist organizations, capabilities, and intentions; and
- build technology-based tools for better threat assessment and management.

With DICTUM, the nation could better interpret indicators of terrorist activity—especially in situations with high signal to noise ratios; formulate effective responses; and anticipate future problems. We propose the investigation and formulation of alternate logical frameworks for analysis, drawing heavily on expertise in the social sciences and incorporating rationales reflective of terrorist thinking. In addition, DICTUM includes means to test the robustness of analyses to differing assumptions about initial and bounding conditions, scenarios, and logic.

Coupling expert understanding of human behavior with fundamental systems analysis, engineering and physical sciences, computation power, and data exploitation and visualization, would yield models and tools to simulate terrorist behavior. These models, validated against historic case studies of terrorism, would provide input for those involved in monitoring, tracking, and providing homeland security. They would also suggest capabilities that could effectively disable or deter known or potential terrorists. Eventually, the models might be able to predict terrorist behavior before it occurs—or at least identify a spectrum of threats that is narrow enough to enable preventive measures. DICTUM aims to enable recognition, anticipation, and deterrence of terrorist behavior.

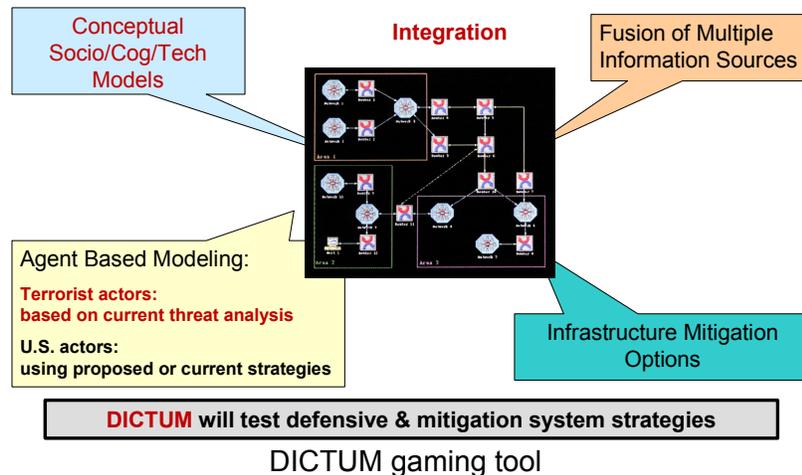
Studies of past terrorist behaviors suggest certain indicators of suspicious behavior patterns. The example here indicates the importance of integrating information from data exploitation,

systems analysis, and social network analysis with a cultural and contextual understanding.

*Example.* The Immigration and Naturalization Service records four groups of foreign nationals entering the U.S. within a week of one another, all coming from different cities in Asia. Each group goes to a different American city. A comprehensive data system, equipped with pattern recognition tools and integrated information systems, goes on alert to track their monetary transactions before and during travel. Financial analysis shows that all of the airline tickets were paid for from a single foreign bank account. Further financial analysis shows that although members of the groups are making credit card purchases in different names, all of the balances are being paid out of another single foreign bank account. Telephone records indicate that these groups are making many long-distance calls to one another and to sites in Asia, but very few local calls, indicating that they are “social isolates” in the U.S. The various indicators are positive for potential terrorist activity. Yet they could also be indicative of an Asian team for the Olympics coming into the country. Further social network analysis could reveal the additional indicators necessary to adequately characterize the group. That information can be fed to data exploitation systems.

A complete systems analysis approach would call for a “red team” to spoof the monitoring and tracking systems by simulating a terrorist group trying to hide behind a seemingly innocent scenario. Enhanced with learning algorithms, the system could learn over time to modify its pattern searches according to real-world and simulated inputs.

DICTUM would add gaming and adaptive, dynamic social network analysis to data analysis and static network analysis. Rigorous systems analysis of historical terrorist behaviors, coupled with knowledge and theoretical models from the social and cognitive sciences, would form the basis for integrated conceptual models and frameworks for analyzing terrorist behaviors. Simulation tools would then allow gaming run in multiple formats for multiple purposes, e.g., validation of theories (using historical data sets), learning, decision analysis, and prediction.



## Technology Challenges

The challenges are both technical and cultural. First, this is a hard computer science problem involving multi-disciplinary data fusion, integrity, exploitation, and visualization. The relevant data sets and knowledge are from multiple disciplines with a wide range of formats. They have been collected with varying degrees of rigor using discipline-dependent methods. Analysis of the data and information would benefit from sophisticated pattern recognition and other computational tools, which have not traditionally been widely utilized in the social sciences.

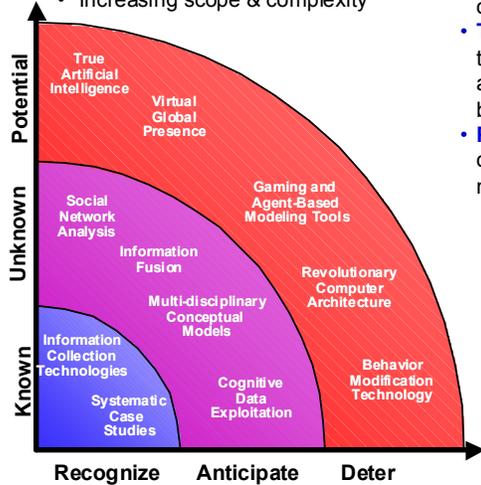
The social sciences are data-rich fields with many interdependent variables and few computational tools by which to systematically analyze and formulate principles. As in other areas, the social sciences tend to be institutionally stovepiped, with little explicit integration among fields and research. This has changed in recent years with, among other things, the interest of the military community in better battlefield management and enhanced human-machine interfaces. Adapting modern data management tools to rigorous analysis of social science data—and data relating to terrorist behaviors in particular—would benefit those who study terrorism as well those in other fields of high priority to national security (law enforcement, military applications, etc.)

Beyond the data management issue, the development of models of behavior and intent—integrating advances in computational modeling with improved social science models—holds great potential providing new insight into this problem.

## The Path Forward

We should pursue this work in two directions

- Increasing capability & intelligence
- Increasing scope & complexity



### Scope

- **The Known:** Already-identified terrorist threats, organizations, actions.
- **The Unknown:** Terrorist threats, organizations, actions that have not yet been identified.
- **Potential:** Terrorist threats, organizations, actions that may not yet exist

### Capabilities

- **Recognize** terrorist activities.
- **Anticipate** terrorist targets, actions, motivations.
- **Deter:** Terrorists before they act.

The short-term goal for DICTUM is to develop a systematic process and tools for rigorous analysis of the behavior of structured, traditional terrorist groups. This will involve development of cognitive data exploitation and analytic frameworks, integrating them with appropriate tools in simulating open systems and networks (such as agent-based modeling). The subsequent challenge would be to model the behavior of loosely organized terrorist groups without regularized operating procedures.

## Conclusion

The ACG will continue to study in depth several of the topics recommended in this report. For the next 5 months the new teams and their goals are:

### *The SDAC (Sense, Decide, Act, Communicate) Team*

Since the concept of an SDAC appeared as a high leverage feature in most of the BHAGs described in the body of this report, the ACG has decided to explore medium-to-long-range concepts, capabilities, & vision for networked SDAC systems and human decision-maker interactions. As part of this study, they will outline the gaps in current technology and identify areas in which Sandia National Laboratories might be able to make distinguishing, transformational contributions toward advancing this concept.

### *The SSB (Smart Secure Borders) Team*

The Smart Secure Borders team is continuing the work outlined in this report, looking for ways that Sandia could contribute to President Bush's vision of "The Smart Border of the Future" that "...keeps pace with expanding trade while protecting the United States and its territories from the threats of terrorist attack, illegal immigration, illegal drugs, and other contraband."\* The team will work closely with other Sandia organizations in pursuit of this goal. In the near term, the U.S.-Mexican border appears to be an especially opportune area for Sandia to begin new work in the border security field. In addition, there may be particular opportunities for Sandia and others to collaborate with the proposed Bi-National Sustainability Laboratory on projects relating to border security.

*\*President George W. Bush, "Securing the Homeland, Strengthening the Nation" (Washington, DC: The White House, Feb. 2002).*

### *The FACETS (Fractal Approaches for Clarifying and Enabling Timely Support) Team*

The FACETS team is working to conceptualize a powerful, fractal based design approach that would enable the multi-user need-tailored tools for rapidly understanding intrinsically foggy situations. This would include attack detection, attack assessment, defense assessment, decision guidance and response. The fractal nature hinges on the themes of Sense, Decide, Act, Communicate that reoccur throughout the threat detect and response system. The system would be dynamic, adaptable, and federated, with the focal point changing as the needs of its numerous members change. The fractal approach of FACETS is based on the belief that there are a common set of inputs, outputs and value added processes that occur or need to occur repeatedly throughout the nation's response system. The design and development of a common architecture would allow these elements to be easily integrated into a dynamic, adaptive system increasing the probability of terrorist event detection and dramatically improving the ability of the nation to respond to horrific events, both natural and man-initiated. In the context of an architecture, fractal implies that the collection of operational units is not predefined or hierarchical and that any "unit" of the structure is similar to any larger or smaller unit in basic function and communication standards. The advantages of a fractal design

philosophy are that it contains common elements and interfaces that scale easily, have self-identifying attributes, and can reorganize as needs dictate.

*The DICTUM (Dynamic Integrated Capability for Threat Understanding and Mastery) Team*

The goal of DICTUM is to understand how an improved national capability for understanding and influencing key decisions and perceptions that underlie terrorist threats to U.S. national security interests might be developed. To this end, the team will assess relevant organizational, historical, and social science models/analogs for terrorist behavior and the role for computational tools in the development of this capability. The study will focus on the viability of integrating tools such as social network analysis and agent based modeling to understand the behavior of terrorist organizations in various environments.

The results of this next phase of our study will be available in a report in the fall of 2002.