ORGANIZING "VIRTUALLY"

Facilitating Effective Homeland Security through DoD's JC4I System

Major Isaiah Wilson III, Ph.D.
United States Military Academy
April, 2002

The views expressed in this paper are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense or U.S. Government.

INTRODUCTION[1],[2]

> *We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.*

> *In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself. A dependence on the people is, no doubt, the primary control on the government;but experience has taught mankind the necessity of auxiliary precautions.*

> [A]merica will do what is necessary to ensure our nation's security. [H]omeland security will make America not only stronger but in many ways better. Knowledge gained from bioterrorism research will improve public health. Stronger police and fire departments will mean safer neighborhoods. Stricter border enforcement will help combat illegal drugs. [A]nd as government works to better secure our homeland, America will continue to depend on the eyes and ears of alert citizens.

The quest for ensuring a secure, but free society in the United States continues to this day. The attacks on the American homeland on September 11, 2001 shine a particularly stark light on the issue. The attacks on the homeland have shaken America's sensibilities regarding what is and what is not proper use of the active military within the territorial boundaries of the national state. In fact, the new sensibility is that DOD *must* have a direct role in executing the six functions of homeland security iterated by President Bush in Executive Order 13228 – detection, preparation, prevention, protection, response, and recovery.[3] The fledgling Office of Homeland Security (see figure 1 in appendix) continues to struggle with the implementation of the policy. The office, empowered to "coordinate and facilitate" rather than command and control federal, state, and local HLS efforts, has left the office and its Director, Governor Tom Ridge, hamstrung.

While the moment of the crisis has aided in a collective effort so far, the over 46 disparate agencies maintaining a stake and a market share in HLS have already begun to buck under the loose yoke Ridge and OHS has placed upon them. While nothing short of patriotism drives these agencies in their efforts to better secure the homeland, their different understandings of the issue, different organizational cultures, different point of view on the subject, different capabilities available to bring to bear on the subject – all contribute to a less-than-effective (and less than efficient) collective effort. Turf battles are already well underway.

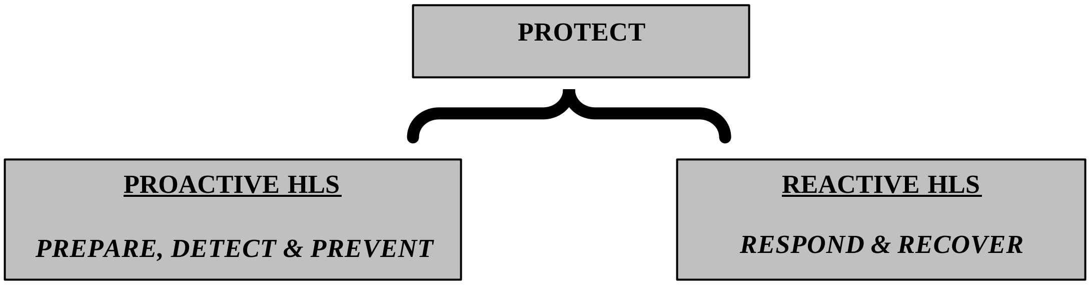
Organizing at the regional level (operational-level in military parlance) has so far centered on the simple, but effective, premise of sticking with what already works. The longstanding first-response relationships that already exist between the "Big Five" – the Federal Emergency Management Agency (FEMA), the Federal Bureau of

Investigations (FBI), Immigration and Naturalization (INS)/Border Patrol, US Customs, and the Department of Defense (DOD) – form the baseline of cooperative planning and action for HLS at the regional level.[4]

More can surely be done to better these relationships. Some "brick and mortar" organizational re-structuring has taken place. However, physical restructuring alternatives are wrought with potential problems (threat to the Federalism "balance"; congressional naysaying to radical agency "tear-away" options; public concerns of Leviathan[5]-like government; etc.). Better solutions for a more effective multi-agency coordinated effort in HLS implementation most likely lie in other alternatives.

Organizing "Virtually"

It is useful and accurate to categorize the six functions of homeland security in the following manner:



The physical structures and informal, experience-based relationships that already persist find the United States well organized for "reactive homeland security." The President, the nation, and its citizenry, however, are no longer satisfied with just a respond and recover approach to HLS – the scope, scale, and nature of the attacks of 9/11 elevates the strategic risk inherent in a reactive strategy far too high. The challenge to Governor Ridge, the Office of Homeland Security, and the "Big Five" lead agencies is how to organize, structure, command and control for implementing a "proactive" HLS strategy. One alternative seldom if ever considered is the "virtual" option. Building an electronic, information technology (IT)-based *system of systems* architecture that can enhance coordinated efforts horizontally (governmental, non-governmental; private, and public) and vertically (federal, state, and local), without disrupting physical structures is an approach with great potential for improving national reaction time. More importantly, this architecture can enhance "intelligence"[6] gathering and analysis across the spectrum of responsible agencies, providing OHS and the nation with a proactive capability that allows for an effective corroborative effort in preparation, detection, and prevention against future assaults on the nation.

The experience and infrastructure that the Department of Defense (DOD) maintains in its command, control, communication, computers, and intelligence systems (C4I) can provide the baseline for this virtual organizational architecture. The commander, USNORTHCOM will be responsible for enabling the HLS mission through the infusion of this C4I system into HLS operations.

What is C4I?
How can it contribute to HLS?

Better intelligence is the key to proactive homeland security. Command, control, communications, computer (C4) systems are the joint (multiservice) force commander's principle tools used to "collect, transport, process, disseminate, and protect data and information."[7] The joint force commander controls the C2 system to ensure that data and information get to the right place on time and in a form that is quickly usable by its intended recipients and generates appropriate actions.[8] This, in turn, helps provide a *common operational picture* (COP) of the situation (crisis, threat, normal operations, etc.) shared by all members of the joint force team and enhances the processing of disparate information and data from different sources into reliable and pertinent intelligence. C4I systems provided through the USNORTHCOM joint force commander could provide the critical link between the Office of Homeland Security, the regional level lead agencies, and first-responders. That is, DOD can and should have a crucial role and mission in linking together the ends, ways, and means (strategy)[9] through C4I systems to ensure a timely, proactive approach to homeland security (see Figure 2 in appendix).

The challenges facing the new NORTHCOM commander boil down to three "realities:"

- The Commander, US Northern Command will not have Combatant Command (COCOM) authority over non-military assets in HLS. As a result, the commander is challenged by having to translate its traditional powers of "command and control" (C2) into an effective tool of "coordination and cooperation."
- "Plugging-in" without "overloading" the capacity of civilian agencies and organizations dominating the HLS mission. Figuring out how to fuse joint military C4 systems into a civilian infrastructure (hardware-wise, software-wise, and procedurally) is a challenge facing the commander.
- Sharing IT capabilities and know-how horizontally and vertically while preserving conditions for future military operational security and non-proliferation of Information Operations (IO) capabilities is a critical challenge facing the commander, USNORTHCOM.

Conceptualizing the C4I System Architecture for Homeland Security
Ensuring a Common Operational Picture through "Virtual" Organization

The CJCS' "The C4I For the Warrior" concept establishes a twenty first century vision of a global information infrastructure comprised of a web of computer controlled telecommunications grids that will transcend industry, media, government, military, and other nongovernmental entities.[10] The grid networks will support both vertical and horizontal information flow to joint and multinational forces (See Figure 3 in appendix). The C4I system for the

Warrior architecture also provides a revolutionary Decision Support System (DSS), that is designed to synchronize and enhance connectivity in the functions of joint and multinational reporting, intelligence, and logistics.

Translating this sort of electronic information-sharing architecture to homeland security is a key challenge for Governor Ridge's office and the commander of USNORTHCOM. Where the joint C4I *For The Warrior* system (C4IFTW) connects multiple military services and various nations in joint and multinational operations, the system architecture could either be modified to accommodate HLS civilian agencies or used as a model for the creation of a similar architecture based on the HLS mission. The Global Command and Control System (GCCS) could serve as a model for the design of a similar system that provides inner-connectivity between OHS efforts at the national/strategic level (federal level) and agency efforts at the "theater" (state and local) level. As an interim solution, this joint military architecture could be adopted as the HLS architecture. This later option, however, would require a restructuring of FEMA or some other appropriate lead agency to play the typical "JTF" role; the system would require re-tooling to effect a "coordinate and cooperate" operational schema. The difficulty in leveraging the full potential of the military's C4 system in HLS will lie in the USNORTHCOM commander's designation as a "supporting" agency. The usual planning, scheduling, resourcing, and sustaining functions that are part of the command and control (C2) element of the C4 system would need to be delegated to FEMA. These functions will have to be translated into in a "coordinating and cooperating" context. The difference is more than a semantic one.

Opportunity and Challenges in Communication and Communication Technology.

Federal, state, and local agencies are working to create compatible and attack-resistant communication systems to gird against future terrorist attacks on the United States. With the exception of FEMA and DOD, the federal government, as well as state and local agencies, has a lot to learn about wireless communication alternatives.[11] The Department of Defense engaged in a long-term effort of replacing incompatible legacy systems with flexible, interoperable communications technologies years before the cataclysm of 9/11. One system well underway in the defense acquisition process is the *Joint Tactical Radio System.* The acquisition program calls for the construction of up to 180,000 common radios for the US Army, Navy, Air Force, and Marines, with fielding to begin by 2007. These software-defined radios combine computer processors with radio transceivers to mimic a variety of existing radio systems.[12] The wisdom in this kind of system architecture greatly enables the efforts of civilian agencies such as police, fire and emergency medical departments in response to large-scale disaster. This sort of multi-functional communications medium could bridge reactive and proactive HLS efforts across multiple jurisdictions, bypassing organizational stovepipes and "hard-wired" communications networks.

Another example is found in the Air Force's *ReadySet* system. This device is a tactical switch with router and hub that can connect most types of radios to the public telephone system or even to voice-over-Internet technology. First-responders from numerous agencies can be "plugged into" this system, making their otherwise incompatible communications mediums interoperable with military networks.[13] The US military (joint force commander, USNORTHCOM) will also have at its disposal continuous operations platforms that can be employed either as a more secure supplement to normal communications networks or as a replacement when traditional systems and networks fail or are destroyed in attacks. Airborne Command, Control and Communications (ABCCC) platforms could greatly enhance multi-agency operations in homeland security, particularly when combined with any of the fusing-type technologies mentioned earlier.

The challenge to the unified commander remains the concerns with operational security and protection of defense-related technologies from proliferation, lingering difficulties in expediting the acquisition process to realize some of these connecting technologies in a timely and therefore useful time period, and the problem of allowing civilian agencies to "command and control" military communications systems. These challenges are daunting but not insurmountable.

Opportunity and Challenges Regarding Computer Technology.

The three central components of computing for homeland security are *continuity of operations, information assurance, and collaboration*.[14] Computer technology is the *Achilles* of the homeland security battle, "bringing strength and armor, but also vulnerabilities."[15] The White House's homeland security budget is aimed at many programs that focus on exploiting American computing strength while defending computers from attack. The capacities in computer IT and wartime-use that DOD and the new USNORTHCOM can bring to this new fight are unbounded. The technology has been well integrated into military doctrine, tactics, techniques, and procedures (operational ways) for decades, and has survived the test of combat. What is similar between this new HLS fight and combat of the past make the fusion of these military-based capabilities valuable to the HLS mission. However, the differences between the old way and the new way of war present significant challenges to the USNORTHCOM commander. When the fight is (1) on the homefront and (2) as much a virtual, informational warfight as it is a physical one, peculiar difficulties in effectively prosecuting the war arise. Sharing the technology, the systems, the standard operating procedures with a multitude of civil and private entities has the potential of wreaking havoc within the traditional military paradigm of warfighting. Operational security and protection of the military's ways and means of warfighting must be reconceived. Strategic, operational, and tactical risk must be assessed and managed in a totally different manner.

Though the military's processes and procedures for doing business may prove more efficient and more effective than civilian or private counterparts, the civilian community (private industry) has a significant jump on DOD in terms of IT development. A challenge for the combatant commander will be in "plugging in" old legacy military systems into state-of-the-art commercial systems owed and operated by many of the other 46 agencies taking part in HLS. Catching up with *this revolution in technological affairs* is a near-term challenge the unified commander will have to face and overcome.

Another challenge facing the new military command is the challenge of enabling the right access, to the right players, while denying that access to "others." Cybersecurity is a challenge because of the borderless character of the subject of concern – information. Unauthorized users are one problem. Identifying misuse of computer systems by authorized users is another, and probably the greater challenge of the two. Defending against the "threat" takes on another peculiar aspect, when more often than not in homeland security, what we face is a "threat from within" . . . perhaps an enemy from our own ranks and community. It is this very sort of threat that the nation's Founders had in mind when they institutionalized the citizenry's healthy skepticism against standing armies. The concern was not with a standing force; it was more with *where the army could and should stand*. The use of active military forces, on American soil, against an "enemy from within," is a scenario the nation has hoped to avoid and one that the government has strictly regulated through laws, statutes, and conventions. The exception to these restrictive regulations has typically been in domestic crisis situations, or what has earlier been identified as "reactive homeland security." Finding a need for a more proactive HLS challenges all those earlier founding principles that have up until now erred on the side of liberty rather than order in the use of the military within the continental United States. The establishment of USNORTHCOM marks the end to this sort of civil-military separation, raising new concerns with the balance between the government's need for access to private citizen lives and information, and the citizenry's right to privacy. The cleavage between these two ideals is the nation's center of gravity in this new war. It is not surprising that the enemy – from without and from within – has focused attacks at that cleavage point. How to close that gap and protect that informational center of gravity without damaging it ourselves in the process is the paramount challenge facing the Office of Homeland Security and the future commander of USNORTHCOM.[16]

Challenges to HLS Information Operations

Case Analysis: Computer Network Operations (CNO)

Information Operations (IO) are defined as *actions taken to affect adversary information and information systems while defending one's own information and information systems.*[17] One element of IO is computer network operations (CNO). CNO is also divided into two mission types: computer network attack (CNA) and computer network defense (CND). Time and space restrictions in this essay prohibit a detailed explanation of these different forms. However, CNO does provide a relevant case to illustrate some of the more prevailing challenges facing OHS and USNORTHCOM as they struggle with integrating these types of operations into homeland security.

Computer network attack (CNA) consist of "operations that disrupt, deny, degrade, or destroy information resident in computers and computer networks."[18] CNA includes the targeting and physical destruction of computers and networks. Traditional understanding of these types of offensive operations derive from the understanding that enemy lines of operations and communications (LOOs and LOCs) will be separate from one's own lines. In HLS, this is not the case. Confusing the issue even further, these lines of communication are not "for military-use only." These LOCs are the lines of everyday, normal commercial and public operations. Except in absolutely dire situations, physical attack on computers and networks would equate to attacks on the nation's own people and resources -- facts rendering this option unacceptable in most cases. Even more passive actions taken against these communication systems would degrade normal US operations, commercial activities being the most important among equal domestic (global) functions.

The CND capabilities the unified commander can bring to the issue area are less invasive than CNA operations. In fact, it is in computer network defense that USNORTHCOM can leverage its C4I systems most effectively. USNORTHCOM can greatly enhance the homeland security effort in the area of information security (and therefore, *information assurance*). The main superhighway remains the Internet. The US defense community maintains at least three additional electronic "highway" systems. These networks are stair-stepped by varying degrees of classification (unclassified, FOUO; Secret; and Top Secret, SCI).[19] These classified information highways "could" provide the homeland security community with "secure travel." Sharing these network capabilities and allowing non-governmental, private, state and local entities access to these byways remains the key inhibitor to what could prove to be a necessary and sufficient enabler of a common operating picture and paradigm, and therefore a more effective approach to homeland security. The risk to future traditional military operations security, however, may prove too much for the unified commander to overcome.

Another element of CND operations is early-warning and alert notification. DOD has several early warning and alert processes already in use. Information Assurance Vulnerability Alerts (IAVAs) are bulletins that permeate the defense community, in an attempt to raise defense community awareness of potential threats. DOD also maintains a new five-level INFOCON system, intended as a system that incrementally and rationally categorizes threat escalations, allowing for agencies to match appropriate treatments against increasing threats. Two problems persist with these systems that plague the USNORTHCOM commander with more challenges. The IAVA system suffers from a compliance and dissemination problem. IAVAs often do not reach the tactical (first-responder) level (or at least not consistently so). In terms of the INFOCON system, at present there is no connectivity between this system and OHS's five color-coded levels of domestic security.[20]

There are ten other distinct "elements" to Information Operations. Each offers useful capabilities to the HLS mission. Each are plagued by civil-military fusion problems.

CONCLUSION

> Before you can collaborate, you have to come up with consistency in how
> you model information. You need common data models, common data
> definitions, common standards.[21]

Cooperative ventures abound between DOD (the military) and the rest of the Homeland Security community. The establishment of a new unified command, USNORTHCOM, is testament to the nation's commitment to an effective HLS fight. The military's mission-oriented culture, organizational designs, and technical capabilities – if fused rightly with the myriad of other civilian agencies in the HLS "command" – can prove to be critical enablers of a more effective, proactive HLS strategy.

Successful integration will depend on transforming the military from a supported, "command and control" – based organization to an organization comfortable in a supporting, "coordination and cooperation" role. The commander of USNORTHCOM will have to overcome much institutional inertia in the areas of OPSEC and protection ("hoarding") of IT assets, if information sharing is to occur, laterally and vertically throughout the HLS community. "Plugging in" to homeland security without threatening other agency jurisdictions and without damaging citizen's sensibilities regarding appropriate roles and missions for military forces is the challenge. In that sense, it is a challenge very similar to that which faced the nation's Founders as they struggled with balancing freedom with order (liberty with security). The charge to this new commander will be the same as it was to those Founding Fathers . . . to ensure that the government remains a nation designed *of the people and for the people*.[22]

SOURCES CONSULTED

"Advanced Search Technology Prompts Privacy Concerns," *Defense News*, 1-7 April, 2002, pg. 2.

"Agencies Accelerate Communication Compatibility Efforts," *Defense News,* 1-7 April, 2002, pg. 4.

"Cyber-Security Team Guards IT Infrastructure," *Defense News,* 1-7 April, 2002, pg. 10.

Gaddis, John L., *Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy,* New York: Oxford University Press, 1982.

Hoge, James F., Jr., and Gideon Rose, *How Did This Happen? Terrorism and the New War,* New York: PublicAffairs, 2001.

Ignatieff, Michael, *Virtual War: Kosovo and Beyond,* New York: Henry Holt and Company, 2000.

"IT Is Vital Cog in Homeland Spending Plan," *Defense News*, April 1-7, 2002, pg. 2.

Jensen, Geoffrey and Andrew Wiest (eds.), *War in the Age of Technology: Myriad Faces of Modern Armed Conflict*, New York: New York University Press, 2001.

Journal of Homeland Security, ANSER Institute for Homeland Security, *World Wide Web, accessed at* www.homelandsecurity.org.

Larson, Eric V. and John E. Peters (eds.), *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options*, Santa Monica, Ca.: RAND Corporation, 2001.

Lowi, Theodore J. and Benjamin Ginsberg, *American Government: Freedom and Power*, New York: W.W. Norton & Company, 2001.

Office of the Chairman of the Joint Chiefs of Staff, Joint Pub 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, 30 May 1995.

Office of the Chairman of the Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations,* 9 October 1998.

O'Hanlon, Michael, *Technological Change and the Future of Warfare,* Washington, D.C.: Brookings Institution Press, 2000.

"Pentagon Eyes Homeland Command," *The Washington Times,* [On Line], accessed at www.washtimes.com, 28 January 2002.

"Programs Juggle Computer Utility, Security Concerns," *Defense News*, 1-7 April, 2002, pg. 4.

Rosen, Stephen P., *Winning the Next War: Innovation and the Modern Military,* Ithaca: Cornell University Press, 1991.

Rossiter, Clinton, (ed.), *The Federalist Papers: Hamilton, Madison, Jay,* New York: Penguin Books, 1961.

"Technology Drives Border Security Agency Initiatives," *Defense News,* 1-7 April, 2002, pg. 6.

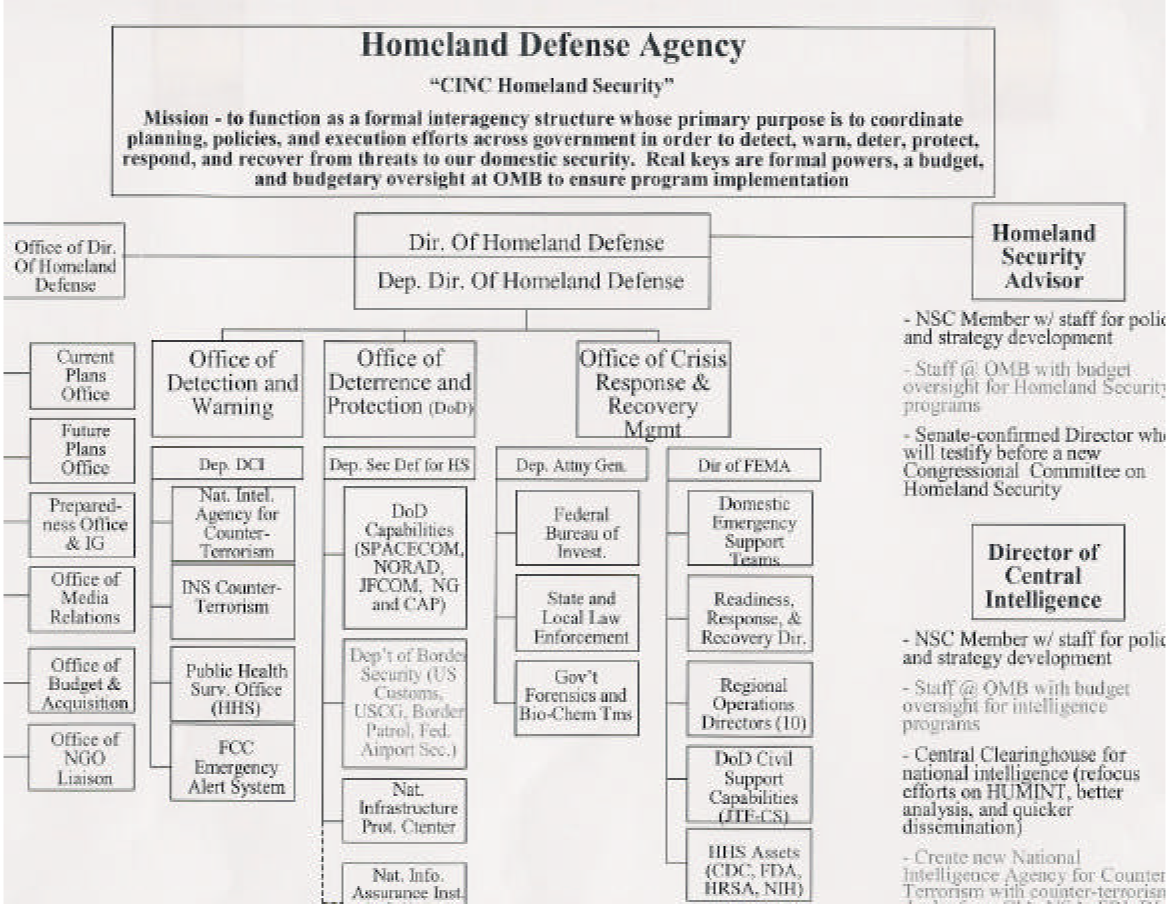
United States Army, FM 3.0, *Operations*, 2001.

Wilson, Isaiah, III, Researcher and working group notes, *Interagency Working Group of Organizational Issues for Homeland Security,* Office of Homeland Security, September 2001 to April 2002.

APPENDIX

FIGURE 1.

The following is a graphic depiction of the Office of Homeland Security.


Homeland Defense Agency
"CINC Homeland Security"
Office of Dir. Of Homeland Defense
Dir. Of Homeland Defense
Dep. Dir. Of Homeland Defense
Homeland Security Advisor
Current Plans Office
Future Plans Office
Prepared-ness Office & IG
Office of Media Relations
Office of Budget & Acquisition
Office of NGO Liaison
Office of Detection and Warning
Dep. DCI
Nat. Intel. Agency for Counter-Terrorism
INS Counter-Terrorism
Public Health Surv. Office (HHS)
FCC Emergency Alert System
Office of Deterrence and Protection (DoD)
Dep. Sec Def for HS
DoD Capabilities (SPACECOM, NORAD, JFCOM, NG and CAP)
Dep't of Border Security (US Customs, USCG, Border Patrol, Fed. Airport Sec.)
Nat. Infrastructure Prot. Ctenter
Nat. Info. Assurance Inst.
Office of Crisis Response & Recovery Mgmt
Dep. Attny Gen.
Federal Bureau of Invest.
State and Local Law Enforcement
Gov't Forensics and Bio-Chem Tms
Dir of FEMA
Domestic Emergency Support Teams
Readiness, Response, & Recovery Dir.
Regional Operations Directors (10)
DoD Civil Support Capabilities (JTF-CS)
HHS Assets (CDC, FDA, HRSA, NIH)
Director of Central Intelligence

Mission - to function as a formal interagency structure whose primary purpose is to coordinate planning, policies, and execution efforts across government in order to detect, warn, deter, protect, respond, and recover from threats to our domestic security. Real keys are formal powers, a budget, and budgetary oversight at OMB to ensure program implementation

Homeland Security Advisor

- NSC Member w/ staff for polic and strategy development
- Staff @ OMB with budget oversight for Homeland Security programs
- Senate-confirmed Director wh will testify before a new Congressional Committee on Homeland Security

Director of Central Intelligence

- NSC Member w/ staff for polic and strategy development
- Staff @ OMB with budget oversight for intelligence programs
- Central Clearinghouse for national intelligence (refocus efforts on HUMINT, better analysis, and quicker dissemination)
- Create new National Intelligence Agency for Counter Terrorism with counter-terrorisn

Source: Office of Homeland Security (November 2001).

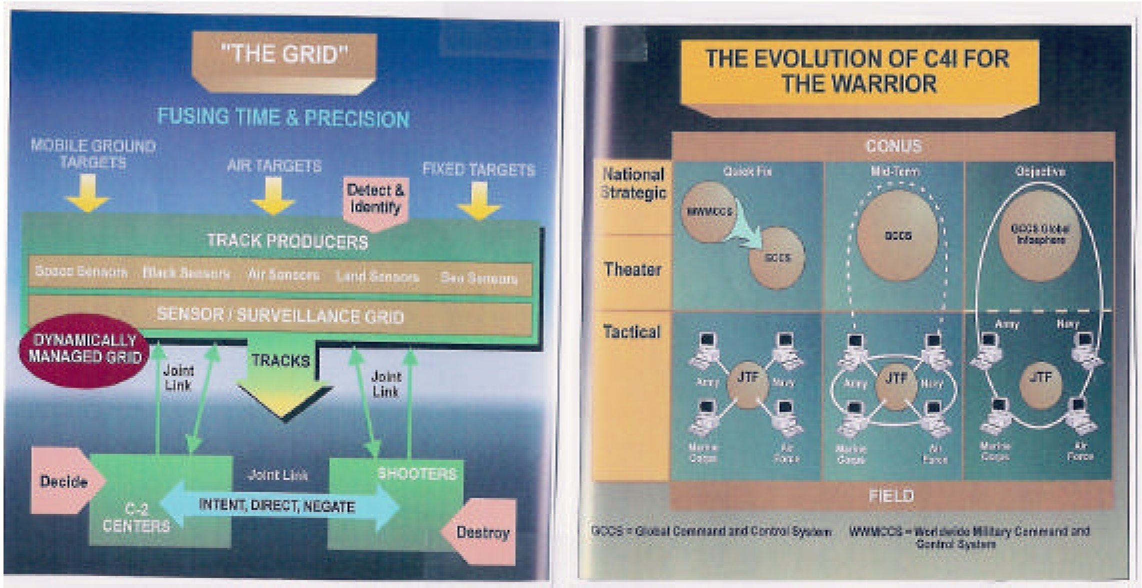
FIGURE 2.

The following chart summarizes the C4 system, its objectives, and its configuration for wartime scenarios. The chart then translates these military wartime factors into HLS context, identifying some of the "challenges" facing the new combatant commander.

	TRADITIONAL WARTIME SCENARIO/CONTEXT	NEW HLS WARTIME SCENARIO (TRANSLATION) ("CHALLENGES")
OBJECTIVES	· Provide authorities at all levels and functions with timely and accurate data and information · Provide unity of effort · Exploit "Total Force" Capabilities · Properly Position Critical Information · Information "Fusion"	In general, the same OBJECTIVES, with the following caveats: · A supporting, rather than a supported command. Can provide assets and processes to "facilitate" enhanced unity of effort, but cannot ensure unity of effort. · "Total Force" capabilities must include state and local (even community) capabilities. Knowledge of, access to, and synchronization of these civilian assets into the joint C4I system is a challenge · Placement of assets and capabilities remains a plausible and effective function/objective · Information fusion → a challenge due to security classifications of portions of the military C4I system. A "sharing" problem (stovepipes)
SYSTEMS CONFIGURATION	· Configured and operated to meet the requirements of interoperability and the command being served, with priority to the National Military Command System (NMCS). · Terminal Devices (telephones, faxes, computers) → transform information. · Transmission Media: connect terminal devices (radio, metallic wire, fiber-optic cable, space-based systems). · Switches: route traffic through a network of transmission media (circuit and message). · Network Control: provide management of area, regional, theater, or global networks (long haul transmission centers of aggregate/bulk data) · Nodal Control: concerned with the management of local C4 systems (switching systems and terminal devices supporting warriors at locations such as command centers or C2 facilities.	· The "command being served" will be FEMA or some other *civilian* agencies (fed, state, or local). Priority of configuration will need to go to the Office of Homeland Security (particularly during crisis events) rather than the NMCS. · Lack of both adequate and standardized system architecture within various states and localities.
"COMMANDER" RESPONSIBILITIES	· Command, control, coordination · Submission of C4system requirements · Reporting of incompatibilities among C4 systems · C4 system planning	· Commander, USNORTHCOM will NOT be the "combatant commander" (lead agent) in HLS. · "Coordinate and Cooperate" instead of "command and control"
PLANNING PROCESS	· Combatant commanders review, coordinate, and validate command initiated requirements · Commanders determine C4 system deficiencies · C4 system support is planned and operationally assessed within the chain of command.	· A civilian lead agency (most often, FEMA) will take on primary responsibility for HLS planning at the regional (operational) level. · DOD systems under the control of civilian agencies (turf battles and compatibility problems · OPSEC and Non-proliferation of military IT systems and capabilities
EMPLOYMENT PRINCIPLES	· Establish liaison early · Leverage limited C4 resources · Standardize operating principles · Agree on policy in advance of war · Use US interpreters · Use common cryptographic systems · C4 systems are designed to support wartime scenarios	· Synchronize federal, state, local, governmental, non-governmental, public, and private operating principles and procedures with the military C4 system SOPs · Need for US military "interpreters" for translation of C4 system to civilian agencies both horizontally and laterally. · Sharing of cryptographic systems, horizontally and vertically. Proliferation concerns. Interoperability concerns.

FIGURE 3.

The following graphic describes this concept, as conceived for traditional JTF “warfighting” scenarios.



"THE GRID"

THE EVOLUTION OF C4I FOR THE WARRIOR

Source: Joint Pub 6-0 (30May 1995).

NOTES

[1] Quotations from (left to right), the Preamble to the United States Constitution (from Lowi and Ginsberg, *American Government, sixth edition,* New York: W.W. Norton & Company, 2000); James Madison's *Federalist Paper #51* (See the Clinton Rossiter edition of *The Federalist Papers,* New York: Penguin Group Publishing, 1961); and President George W. Bush's *State of the Union Address,* 29 January 2002.

[2] The President is expected to soon sign into law, the Unified Command Plan (UCP) creating a new combatant command responsible for homeland security (HLS), US Northern Command (USNORTHCOM). USNORTHCOM will be responsible for providing unity of command and command and control over military efforts related to HLS within the USNORTHCOM Area of Responsibility (AOR) and whose AOR will encompass CONUS, Alaska, Canada, Mexico, and the surrounding water out to approximately 500 nautical miles, to include island territories to include the Bahamas, the US and British Virgin Islands, Puerto Rico, and the Turks and Caicos.[2] The establishment of US NORTHCOM is one of a series of actions taken that marks the evolution of the Homeland Security mission. The USNORTHCOM commander will establish vital operational-level mechanisms necessary and sufficient for the implementation of an effective HLS collective action. The commander will serve as the military's advocate for the defense of the homeland and military assistance to the over 46 different civilian agencies having a stake in HLS. The qualities of the military as an institution and a profession (efficient and hierarchical design, culture of deference to authority, expertise in crisis management and warfighting, and command, control, communication, computers, and intelligence expertise) make DOD and its military services important enabling agencies in homeland security. The "virtual organization" that the USNORTHCOM commander will be able to provide to the Office of Homeland Security (OHS) through its command, control, communication, computers, and intelligence (C4I) system can mitigate much of the problems centering around the issue of how to affect and "effective" collective mult i-agency effort in HLS without traumatizing the constitutional balance between federal, state, local, public, and private. Brick and mortar solutions could jeopardize the delicate balance of Federalism, building a large effective organization that effectively secures the nation, but leaves us with a Leviathan-organization with unwarranted power, less accountable to the public. The C4I challenges facing the USNORTHCOM commander (how to "command and control" in an issue area relegated to "coordination and cooperation"; enhancing multi-agency interoperability in information technology (IT) without risking-away military operational security) are daunting, but not insurmountable. Nesting USNORTHCOM C4I potentialities into the broader HLS mission, through a strategic-operational process, and teaching the command to "coordinate" from a supporting agency role, can greatly enhance the efforts of all agencies with a role to play in HLS.

[3] Executive Order 13228, Establishment of the Office of Homeland Security, 8 October 2001.

[4] Relationships in crisis response and recovery are well-developed. The informal coordination between the ten (10) FEMA regions, the two (2) Continental United States Army (CONUSA) regions, and the fifty-six (56) FBI regional field offices seem to satisfy two of the six HLS functions rather well. Information collected from various sources as part of a six month informal interagency working group tasked by Governor Tom Ridge (Director, OHS) to consider alternatives for homeland security organization. This author was a participating member of that 2001-02 working group.

[5] See Thomas Hobbes' *Leviathan.*

[6] Defined as 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas, and 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. See FMs 34-1, 34-10, and 34-40 for more on military intelligence. The problem inherent in intelligence operations in homeland security lie in the difficulty of identifying and dealing with an "adversary" that more often than not is "from within," and the collection of "intelligence" from private US citizens.

[7] Joint Publication 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, 30 May 1995, vii.

[8] Ibid.

[9] "Strategy" is popularly defined as the relating of ends (goals), ways (operational and organizational processes and procedures) and means (resources and capabilities). John Lewis Gaddis provides a more nuanced definition, defining strategy as "the process that relates ends to means, intentions to capabilities, and objectives to resources." See Gaddis, *Strategies of Containment*, (1982, vii.)

[10] Joint Publication 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, 30 May 1995, pg. II-11.

[11] Arthur Hill, Strategis Group, March 13 2002 interview with *Defense News*.

[12] "Agencies Accelerate Communication Compatibility Efforts," *Defense News*, 7-10 April 2002, pg. 4.

[13] Ibid., pg. 8.

[14] Steven Cooperman, Director of Homeland Security Solutions for Oracle Corporation, Reston, California. *Defense News*, April 1-7, 2002.

[15] James M. Gifford, "Programs Juggle Computer Utility, Security Concerns," *Defense News*, 7-10 April 2002.

[16] This is one of the contributing arguments Congress has considered in its arguments for a Department of Homeland Security rather than (or in addition to) an Executive Office staff agency. President Bush's June 7th proposal for a Department of Homeland Security appears to recognize the power balancing dilemma inherent in organizing for homeland security, seeking a new equilibrium through a cabinet organization subject to the overwatch and regulation of both the executive and legislative branches. How this new development will affect DoD's new combatant command remains to be seen.

[17] Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October, 1998, pg. vii. This definition is currently under revision. However, until release, the definition used here remains the official joint military definition.

[18] Field Manual (FM) 3.0, *Operations*, U.S. Army, 2001, chapter 11, page 18.

[19] For security reasons, details of these networks will not be discussed in this paper.

[20] Information garnered from a Q&A session with a staff officer (name held confidential) representing Joint Task Force-Computer Network Operations (JTF-CNO), 23 April 2002. Also see "IT is Vital Cog in Homeland Security Plan," *Defense News*, 7-10 April 2002, pg. 2.

[21] Steven Cooperman, Director of Homeland Security Solutions, Oracle Corporation, *Defense News*, 7-10 April 2002, pg. 8.

[22] Abraham Lincoln, *Gettsyburg Address.*