Homeland Security and Defense:

Potential Dilemmas vis-à-vis Weapons of Mass Destruction, Immigration, and Telecommunications/Cyber Warfare.

A summary paper for the Conference on Homeland Security sponsored by the Denver Council on Foreign Relations.

25 January 2002

This paper was prepared and written by Samuel Spiwak, Graduate School of International Studies at The University of Denver.

Executive Summary

The Fifth DCFR Conference on Homeland Security was held on 25 January 2002. It brought together members of many different sectors affected by the question of homeland security. The conference was divided into three panels which included: (i) Weapons of Mass Destruction and People and Infrastructure, (ii) Immigration, and (iii) Telecommunications/Cyber Warfare. Participants offered dozens of recommendations and observations. There were, however, three distinct themes that were common to all of the suggestions. These three themes were: (i) the need for a systematic approach toward effectively dealing with the problem, (ii) a strong federal agency to coordinate efforts, and (iii) the special role states might play in advancing homeland security.

Introduction: Revisiting the Threat to the American Homeland

On 11 September 2001, the international system was rocked by three separate, yet highly coordinated attacks on the Continental United States (CONUS). Over the course of 90 minutes on that fateful morning, the CONUS shed its cloak of invincibility. It had become clear that while the US was still the only superpower in the international framework, she would no longer be able to ignore active defense of her territory—the continental United States having been free from attack for almost a century and a half.[1] The Denver Council on Foreign Relations (DCFR) has met five times (including this conference) in Denver since an initial meeting was convened at the National War College in Washington D.C. in January 2000 to discuss and analyze the topic of Homeland Defense (HD). The conference on 25 January 2002 focused on three distinct sub-topics

[1] Clearly, the attack on Pearl Harbor in 1941 was tragic and certainly qualified as an attack upon US territory; however, Hawaii was not then a state and did not become one until 1959.

of homeland security: potential scenarios involving weapons of mass destruction (WMD) vis-à-vis people and infrastructure, immigration, and telecommunications/cyber warfare. In particular, this conference focused on the role that HD would play in protecting the state of Colorado in addition to CONUS. This paper summarizes and details the proceedings at the 25 January 2002 Conference on Homeland Security.

Defining Homeland Defense

HD is defined here as the active effort to secure US territory and concomitantly thwart enemy action (both conventional and non-conventional) undertaken by state, state-sponsored, and non-state actors against traditional military and non-military (civilian) targets.[2] It was agreed by the conference participants that HD should certainly be considered under the broad umbrella of national security concerns. The participants also observed that the Office of Homeland Security was not a satisfactory answer to the question of future terrorism against America.[3]

Weapons of Mass Destruction and People and Infrastructure

The panel that discussed Weapons of Mass Destruction and People and Infrastructure (abbreviated here as WMDPI) concluded that there are three distinct and equally important groups of issues that needed to be addressed vis-à-vis WMDPI. There are three groups of issues with respect to WMDPI. These are: (i) HD threats which directly affect states, but are beyond the scope of any one state's capability in the absence

[2] This definition was formulated by the participants at this meeting. A narrower definition had been offered at earlier DCFR meetings in which HD was associated specifically with asymmetric warfare against civilian targets.

[3] At the time of the conference, the Bush administration had not yet introduced plans for a Department of Homeland Security.

of federal assistance, (ii) development of state anti-terrorism plans, and (iii) development of a coherent course of action (COA) for a state to undertake in order to receive a portion of federal funding which is to be allocated to the states in an effort to promote HD at the state level.

Threats to States

Eleven separate points were made with respect to the first group of issues.

First, the United States needs a systemic approach. It is critical that the federal, state, and local spheres work together. This is important for two reasons: (i) effective *and* efficient use of limited resources, and (ii) there are questions of civil liberties and constitutionality, which require substantial oversight.

Second, clearer standards of authority are needed at the state and local levels. The panel called for a greater focus on state-level procedures and doctrine.

Third, participants agreed that greater streamlining and effective use of intelligence *and* interagency cooperation would be extremely beneficial.

Fourth, the federal government needs to redefine its relationship with the media for this war. Effective domestic communications are essential in avoiding panic and unnecessary alarm, calming the nerves of the American public.

Fifth, more money, surge capacity, training, and vaccines are required in terms of public health. Surge capacity is particularly important to cover municipal sports and other publicly attended events, meaning that on any given day, there may be a gathering of tens of thousands of people that are potentially at risk.

Sixth, a number of participants, particularly those with specific expertise in the field, contend that a greater focus on threats to cargo is a critical necessity. A contrast was drawn between the perceived US failure and Israeli success in this arena.

Seventh, the panel determined that it is critical that the public understand that the US is facing a wholly different paradigm following the attacks of 11 September 2001. All phases of American society need to participate together in this wartime dynamic. The administration has, in effect, put the nation on a war footing. Furthermore, an understanding of what is real and what is not is crucial to accurately assessing the situation in the future. Solid efforts in education could help promote the understanding of all. A non-panicked reaction to a future attack might very well lessen the incentive for further attacks.

Eighth, bio-terrorism was discussed in detail. A medical doctor present on the panel briefed the participants on the role biological agents might play in future attacks. Smallpox and anthrax seemed to be the two agents of most concern. The latter is easily distributable in aerosol form and can be spread over a large geographic area. It is not practical to vaccinate large numbers of people. Anthrax is treatable, but only if done so in the early stages after contraction of the disease. Smallpox, on the other hand, is not treatable. Smallpox can be vaccinated against, but there are many practical reasons why mass vaccinations are not a good idea: (i) the vaccinations themselves would likely result in the deaths of anywhere from 1000-3000 people, (ii) not everybody can receive it; for instance, those individuals who have had their immune system compromised as well as those undergoing transplants, and (iii) a shortage of trained personnel at present for administering mass innoculations.

Ninth, the participants decided that even the creation of the Office of Homeland Security had not changed the status quo. FBI and FEMA still investigate potential terrorist threats and no one central office to coordinate and assess potential threats from terrorism has been developed. The panel thought that the current Office of Homeland Security was too weak to accomplish its mission.

Tenth, the panel suggested that ROTC programs across the state (and nation, for that matter) could incorporate certain aspects of disaster response into their curricula. On the other hand, it was pointed out that this incorporation would take away precious time and resources from the ROTC detachment to accomplish their primary mission of preparing cadets for officer commissioning.

Eleventh, participants asserted that a HD headquarters would be an important symbol of resolve and commitment, as one participant had attempted to contact Office of Homeland Security and was unsuccessful after many efforts. A great concern of many of the participants was the current state of cargo security, the panel feeling strongly that an inspection service was badly needed (possibly to be overseen by a new Department of Homeland Security).

State-level Anti-terrorism Plans

The WMDPI panel also concluded that there were eleven key observations on state-level anti-terrorism planning. First, any such plan itself must be comprehensive and be focused on prevention as well as immediate response. Additionally, it is necessary to create an organizational structure or chain-of-command to better facilitate the implementation of a state-level plan. There is currently no organizational structure in place in most, if not all, states.

Second, a careful review of state-level facilities around the country shows how vulnerable the public and private spheres are. Third, state-level "red teams" are needed to assess vulnerabilities. It was suggested that these red teams be covert in nature. Fourth, governors should establish councils of Chief Executive Officers (CEOs) in their states to examine alternative courses of action. These councils would bring the public and private sectors closer together to study homeland-defense issues. This link is important because future terrorism may focus on private business targets (as opposed to political public targets), as they may be easier to strike. The panel decided that state-level plans should attempt to maximize contacts with the private sector for assistance in dealing with the threat of cyber warfare, although some participants were concerned about a potential security breach by sharing sensitive information with the private sector.

Fifth, the plan must recognize that federal funding is transitory. State legislatures should be made explicitly aware of this. A mechanism must be put in place to sustain the level of funding. Participants questioned whether or not state (as opposed to federal) funding could be sought as a way to supplement future need for funds.

Sixth, once the plan has been developed, it must be vetted against other plans that have dealt extensively with terrorism. For example, Britain's experience with the IRA would be a good place to start. The participants suggested that perhaps councils interview town constables in an effort to analyze their effort vis-à-vis local terrorism.

Seventh, states with a large federal (especially military) presence will need to take this into account in developing state-level plans on airspace or ground transit .

Eighth, the primary goal of any state anti-terrorism plan should be to acquire expertise first and assess threats second.

Ninth, education is of key importance to the successful implementation of anti-terrorism plans. The public must be instructed in preventativemeasures and against overreaction. Also, emergency response personnel must be better trained in dealing with the aftermaths of potential disasters.

Tenth, participants discussed volunteerism as an idea that could link the public to the cause of HD.

Eleventh, the panel contended that there exists a dire need for systems, procedures, and policies regarding the media in advance of future catastrophes. Inclusiveness and partnership were buzzwords that were used by the participants.

Courses of Action

Lastly, the panel concluded that there were four key courses of action.

First, seed money is needed for personnel and facilities.

Second, public education and training are required.

Third, funds for a cargo monitoring system are crucial. A pool of equipment is needed with particular emphasis on detection devices. One concern is that there may be one hundred or more miles between the point of attack and the area where equipment is stored. Furthermore, a comprehensive communications system is needed. In particular, this emphasis should focus on standardization (e.g., radio frequencies to facilitate interoperability).

Fourth, the participants considered medical recommendations key in terms of the proposal for federal funds. Among the recommendations considered: more funding for public health, greater funding for public hospitals to acquire (or augment) surge capacity,

increased funding for adequate vaccines and antibiotics to be stockpiled at key locations, education of medical personnel, and education of the public to minimize overreaction.

Summary of WMDPI Panel

The participants offered numerous recommendations at both the state and federal levels. The suggestions generally revolve around three distinct concepts: (i) issues of concern to states that could not be solved without federal assistance, (ii) the development of state HD plans, and (iii) a coherent articulation of reasons for the federal government to appropriate a portion of the funds that have been earmarked for HD to the state level.

Additionally, the panel was concerned that the Office of Homeland Security was not powerful enough to accomplish the goals that the panel deemed necessary to successfully implement HD. Finally, the participants were all in agreement that a systemic doctrinal policy must be put into place for HD to have any chance at future success.

Immigration

The panel decided to focus specifically on state-level immigration concerns. The panel did point out, however, that immigration laws are created at the federal level. Illegal immigration as an issue consists of two parts: (i) how to stem the flow of illegal immigrants and (ii) how to deal with those illegal immigrants that are already in country. Participants concluded that this is primarily an economic issue; many businesses, especially in the agricultural, construction, and restaurant fields, hire a great number of illegal immigrants. There are also many refugees for whom the United States provides a

safe haven. The panel noted the inherent problem in terms of immigration law with the scenario of families of American citizens and illegal immigrants (i.e., grown children of immigrants who by birth are citizens, those married to non-citizens, children born in the United States of illegal parents, etc.). The panel discussed the fact that since 11 September 2001, immigration issues have gained greater urgency. In particular, the panel asserted that current laws (and the current enforcement of those laws) might not be acceptable in a post-9/11 world.

The panel decided that the entire immigration system is in need of an overhaul. Solutions currently being bandied about do not address the causes of the problem; rather they deal solely with the symptoms. INS is understaffed, under budgeted, and under appreciated.

Participants concluded that in order to define immigration issues in terms of homeland defense, it was necessary pragmatically to identify the threats posed by illegal immigration. America will never be able to stem completely the tide of illegal immigration; in addition, panelists noted that it was not just immigrants in general that were the threat, but also those individuals who possessed the intent and capability to act against the US that truly posed the dilemma. The panel thought it extremely important to note that the terrorists involved in the 11 September 2001 attacks all entered the country legally.

One solution is to make the process of obtaining a visa more difficult. Legally, emigrating to the U.S. is a privilege, not a right. The panel felt that is was critical that more time be allotted to consulate members who conducted the interviews of potential immigrants in order to ascertain better their intentions. In addition, the US should require

that the burden of proof rest with the immigrant in terms of character, background checks, criminal history, etc. and allow time for follow-up on these verifications. The panel also noted that the interviewing position does not carry a great deal of prestige. As a result, individuals assigned to those positions are often not of the highest caliber; certainly not possessing capabilities commensurate with the importance of their positions. The panel asserted that giving these positions the pay and prestige the position demands would go a long way in the fight against terrorism toward increasing the utility of the interviewing position.

The participants stated that the INS was under funded and as such it was nearly impossible to conduct its mission with any reasonable hope for success. The INS operates primarily on the borders and at major ports of entry; however, it is not possible, in the opinion of the panel, for the INS also to monitor the whole of the interior of the United States. In addition, US agencies (in general) and the INS (in particular) cannot hope to stem the tide of illegal immigration alone. Greater cooperation with other nations is needed (i.e., intelligence sharing, etc.) if the US is to curb effectively illegal immigration into the United States.

The panel discussed the topic of racial profiling as it related to both effectiveness in apprehension of suspects and as a violation of civil rights. Once again, the panel agreed that the best manner by which to deal with this issue was to let the burden of proof reside with the applicant.

The issues of overseas recruitment by universities and lack of enrollment enforcement were also raised. Universities often recruit individuals from other nations as a means to promote understanding among cultures as well as to bring other points of view

to the classroom. However, universities have had some difficulty keeping track of some international students. Individuals who desire to take advantage of this higher-education loophole essentially have been free to do so. One obvious solution to this dilemma is to hold the universities directly responsible for their students arriving and enrolling on time. It seems intuitive that if schools were held accountable for their students' actions (perhaps by a Department of Homeland Security), they would keep closer track of the whereabouts of their foreign students.

The participants discussed the positive economic effects of illegal immigrants for both the United States and Mexico. Certain industries within the US claim they rely upon illegal immigrants to operate their businesses because citizens are unwilling to work for the wages offered. Since these workers will work very hard for very little money, there is little incentive for employers to comply with current laws. The panel suggested that the federal government could link its foreign policy vis-à-vis other countries (those with the largest immigrant pools) in order to help improve conditions within these countries to provide less of an incentive to leave.

One of the main problems with immigration policy concerns families. Once one family member arrives in the US, they often send for the rest of their families. Sometimes the remaining family members immigrate to the US using illegally purchased papers. Generally they intend only to improve their levels of living and, therefore, they are not a matter of security concern; however, panelists noted that immigrants posed a potential threat if they have problems assimilating into the American culture because of such problems as the language barrier, discrimination and prejudice, etc.

As a result of the panel discussion, the participants made ten recommendations: First, the federal government needs to recognize that US immigration policies are outdated. These policies need to be reviewed, particularly in terms of the international environment within which the United States now operates after 11 September 2001.

Second, there is an inherent conflict-of-interest between national security concerns, private business issues, and the unity of immigrant families. Additionally, the interruption of commerce for security reasons (spot checks, inspections, etc) is an enormous issue with which the US needs to grapple.

Third, the panel deemed it crucial that the creation of an entity that is explicitly responsible for issuing visas become a top priority. Furthermore, the panelists asserted the critical nature of satisfactory time allotment vis-à-vis the visa-application process.

Fourth, the government must be sensitive to the views of other minority immigrant groups to any perceived preferential treatment given to Mexican immigrants.

Fifth, the panel asserted the necessity of creating disincentives to small business owners for hiring illegal immigrants.

Sixth, there needs to be a comprehensive Congressional review of immigration policies, endowing the appropriate committee or committees the authority to revise and oversee those changes and modifications.

Seventh, transform university accountability for exchange and foreign students to include, in particular, enforcement via federal agency of new regulations.

Eighth, review current State Department policies vis-à-vis children of illegal aliens being born in this country, particularly in light of new laws and regulations.

Ninth, rethink traditional notions of security through a lens of immigration.

Tenth, the participants contended that no right to immigrate to the US exists; however, immigration is still a privilege. US authorities are thus well within their rights to make laws restricting immigration.

Summary of Immigration Panel

Participants on the panel asserted that there were two key immigration issues: (i) stemming the tide of future immigration and (ii) dealing with the immigrants already in the country. The panel acknowledged that immigration is more often an economic issue rather that a political one. Panelists noted that it was important to consider the current international system in light of the changes that have occurred since 11 September 2001. As a direct result, immigration now needs to be viewed through a lens of national security.

The panelists offered a variety of recommendations. These included: increasing the rigor of the visa process, maintaining tighter control of the university-foreign student relationship, and creating oversight for the process at the Congressional level.

Telecommunications/Cyber Warfare

Some states are behind other states in information security. Participants concluded that there exists a need for a statewide security assessment; however, the panel acknowledged the great cost associated with such courses of action.

Conceptually, cyber warfare has two dimensions. The first is information warfare (IW). IW consists of collecting, analyzing, and disseminating intelligence. The second dimension is strategic information warfare (SIW). SIW refers to countering an enemy

attack upon one's own intelligence capability. The panel concluded that in order effectively to achieve information security, both IW and SIW concerns must be integrated into any solution. This issue must be dealt with at both the federal and state levels. The panel offered sixteen observations or recommendations.

First, a security classification problem exists. If intelligence flows from federal to state authorities, then protection of information sharing becomes a proprietary issue. Therefore, the panel was adamant that a systematic approach to handling security clearances between federal and state officials is needed. Additionally, panelists argued that state officials have an overarching sentiment that federal officials are unwilling to share any more than the very minimum amount of intelligence.

Additionally, participants felt strongly that until there is definitive legal clarification state agencies can expect extremely guarded cooperation by the private sector. Opposition to information classification comes from public suspicion of governmental secrets. The participants offered a recommendation for the security clearance issue, suggesting that adequate information with a limited distribution should be provided for "Heightened State of Alert(s)" issued by Governor Tom Ridge to allow state agencies react rapidly and effectively. The panel also recommended that the commercial sector employ a designated security officer (with federal security clearance) who acts as a liaison between public and private sectors.

Second, the panel believed that more attention directed toward threat assessment is needed with prioritization being the key.

Third, the panel felt that a system of 24 hour operational centers is needed with a specific designated hub to command and control action.

Fourth, participants pointed to a crucial need for cyber-hardening (a process by which computers and information storage units are protected from SIW).

Fifth, some states lag behind others in the critical areas of security and privacy by an estimated five to six years. Some state departments are simply not equipped to deal with these growing concerns, and as demonstrated in the World Trade Center attacks, off-site redundancy is needed for critical data. Efforts to increase security by some states were described by participants as "struggling".

Sixth, while individual state agencies' internal systems may be more secure, most systems have been or are moving to the Internet, where they are more vulnerable to terrorists. Yet, participants noted that many systems are compromised by individuals already within the system. In other words, these individuals have found ways to pursue information or parts of the network that are beyond what they have been allowed access.

Seventh, budgetary and political processes have complicated efforts to assess and protect assets within a state's boundaries. This problem is exacerbated by what participants describe as a "disconnect" between executive- and legislative-branch understandings and priorities. Washington, Virginia, Oregon, and Arizona were identified by panel members as among those states that can serve as models for others seeking to establish comprehensive cyber-security policy regimes.

Eighth, in the event of a catastrophe, whether terrorist attack or natural disaster, some states lack a formal plan for continuity of government. While the issue of governmental succession is addressed within state constitutions, there is no redundancy of critical files. Critical nodes of government, emergency response, and telecommunications may also need to be relocated. The panel offered a solution to this problem: increase mobility of critical functions while also increasing security of current

state facilities and assets. Simulations of physical attacks coupled with cyber attacks and failures should test agency response and preparedness. These simulations should build up to a response plan that will include both the private sector and the state government. Business Executives for National Security have simulations available on their website, and a plan is being discussed, based upon FEMA's plan.

Ninth, critical infrastructure protection and security issues are similar for federal and state governments. The participants suggested that perhaps states should group together to work this issue. Western State Conventions (5-7 state groups) may be an ideal forum in which to produce an appropriate coalition.

Tenth, participants recognized the difficulty to standardizing a comprehensive security structure. Companies do not want to share their internal security process for fear of inadvertently increasing their vulnerability to competitors. This corporate discomfort is exacerbated by the mandated transparency of governmental processes; i.e., once information is yielded to the government it is subject to freedom of information inquiries. The panel asserted that state agencies must determine a manner to protect proprietary information while investigating and reinforcing private-sector cyber security.

Eleventh, panelists recommended that an independent assessment of state-level vulnerabilities to IW and SIW be implemented immediately. Panelists asserted that each potential target analyzed within the assessment must be viewed through both IW and SIW lenses.

Twelfth, participants noted considerable resistance within state governments to providing money and resources for this critical yet embryonic process of identifying resources and priorities. The Info-Guard effort by the Federal Bureau of Investigation

(FBI) could ease this process by providing ready-made spreadsheets for self-assessment of threat and vulnerability. The panel contended that while it fails to protect private-sector assets, perhaps switching to an independent telecommunications infrastructure or network, such as that embodied in the GovNet project, would provide the heightened security that may now be required.

Thirteenth, the participants vehemently argued that education of specific constituencies is the most important aspect of this endeavor. Education is inherently proactive and, once key vulnerabilities are identified, can be a powerful preventative tool. Participants concluded that education is possible with a relatively small monetary commitment. Educating home computer users on security concerns is an untested yet potentially highly effective venue for shoring up systemic security. Home users serve as a ready, unwitting conduit for viruses and worms, along with other tools of the cyber warrior.

Fourteenth, lines of communication must be developed, designed, dedicated, and kept open for response and leadership functions.

Fifteenth, the panel asserted that satellites are a critical vulnerability vis-à-vis SIW. Fundamental technologies lack redundancy. Of the various parts of space-based telecommunications (space and ground control users), it is ground control of satellites that is the least secure.

Sixteenth, states should focus their initial efforts on identifying and prioritizing assets, with an eye to redundancy of infrastructure, critical information, control segments, and Internet Service Providers.

Summary of Telecommunication/Cyber Warfare Panel

Panelists deemed it crucial that any discussion of potential threat posed by the Telecommunication/Cyber Warfare sector include both IW and SIW in its analysis. In continuing a theme echoed throughout the conference, a systemic doctrine was needed as a means of streamlining action and communication among both federal and state actors as well as public and private entities. Participants offered a plethora of recommendations and observations, which included ideas ranging from security clearance procedures to the securing of satellites.

Conclusion: Final Thoughts on American HD

There were three distinct themes that emanated from the 25 January 2002 Conference on Homeland Security. First was the need for a doctrinal approach to resolving the future potentialities of terrorist action at state-and-local levels. Of grave concern to participants was the serious disconnect between the federal and state levels (and also between the public and private sectors).

The second major theme was the essential nature (particularly, in a post-11 September 2001 world) of having a strong federal department to coordinate the multitude of action and bureaucracy that defending America's homeland will entail. The vast majority of the participants did not note a great deal of confidence in the Office of Homeland Security. Finally, it is also up to states to step to the fore and lead HD efforts within and across their jurisdictions.

Conference Participants

As at earlier meetings, participants were drawn not just from the DCFR members, but also from the federal government, the state government, local governments, the private business sector, the press, and universities. The customary DCFR non-attribution rule applied.