Global Business & Development Law Journal

Volume 17
Issue 1 *Symposium Bordering on Terror Global Business in Times of Terror -- The Legal Issues*

Article 14

1-1-2004

# Panel Three: Homeland Defense -- Controlling the Border of Terror Revisited

Lee Zeichner
*LegalNet Works, Inc.*

# Panel Three: Homeland Defense—Controlling the Border of Terror Revisited

## Commentary by Lee Zeichner*

Thank you. During the discussion this afternoon I was thinking of Virginia Wolfe and her book *To the Lighthouse*. Early on the actor describes her husband lovingly as a very smart philosopher but not a brilliant philosopher. She does this by describing that he had been able to work all the way through the alphabet but got stuck on the letter T. He got to Q and he worked his way through Q. Q was difficult but he moved on to R. He managed to get through R and S was, God, he was just stuck on S for the longest time. But he could not make it all the way through and get on to T. I also feel that way when it comes to critical infrastructure, cyber-security, liability, and now Homeland Defense and Homeland Security. I admit I am absolutely stuck on the letter T.

Beginning with the letter A and explaining how we got here, I would like to spend about five minutes and walk you through the history. Most of the history is not well known, but all of it is very much steeped in law, governance and process. As such, it is extremely important to define the parameters of what we are discussing; namely, how does critical infrastructure differ from cybersecurity and how does it differ from Homeland Security. When I say differ, I am asking what are the policy implications? What are the fundamental questions that we must ask? If we are not getting the question right, then chances are we are not getting the solution right as well.

Things really began to change in the aftermath of the Oklahoma City bombing. The first World Trade Center bombing without a doubt forced the government to begin thinking about a new governance philosophy and policy with regard to terrorism. Terrorism was certainly nothing new, but we realized that perhaps the structures we had in place to deal with terrorism were not very responsive. But, Oklahoma City really forced the issue to the forefront. In fact, it scared the Clinton Administration so much, they put together a very senior level task force called the "Critical Infrastructure Working Group" to define new parameters and come up with Presidential level recommendations for how to solve the problem. If you can get your hands on the document, I would highly encourage this. It is a fascinating read. The big theme in 1995 and 1996 was "Critical Infrastructure." We can safely define it as assets in functions and assets in services that are typically owned by the private sector and, if destroyed or

---

* Mr. Zeichner is President of LegalNet Works, Inc., a company that focuses on development of information security laws and regulations with an emphasis on liability, risk management, national security, regulatory compliance, and privacy. Mr. Zeichner has served as senior legal counsel to the President's Commission on Critical Infrastructure Protection and has been a legal consultant to the Critical Infrastructure Assurance Office. Mr. Zeichner also served as legal counsel to the Y2K National Information Coordination Center.

incapacitated, would have an immediate and dramatic impact on national security, the national economic security, or the public's health and safety. Congress incorporated this definition into the USA PATRIOT Act, and it is now being cited. So we really do have something in the letter T. But let's get back to letters A and B.

The Critical Infrastructure Working Group presented their recommendations through Vice President Gore to the President. They came up with essentially five recommendations, which I will not go through, but they really do present the paradigms that we are still struggling with. The first paradigm was that this is an intelligence and law enforcement problem. If we can catch the hackers, if we can catch the terrorists, if we can cuff 'em and stuff 'em, then we are done. We have solved the problem. But guess what? We have institutions and agencies that do that all the time. It is called the FBI, it is called the Intelligence Community, and the Defense Department. So there was really nothing new to talk about.

The second philosophy was that this is really more of a consequence management problem. However, the Federal Emergency Management Agency ("FEMA") already exists. This agency responds when there is a hurricane or tornado and people need to be fed, housed, or clothed. When terrorists attack, the same things happen but from a slightly different angle. Instead of looking before the problem, we really need to focus on what happens after the problem. We need to come up with new and better ways to react and manage the so-called consequences. The only recommendation was to heavily fund FEMA to better enable individuals to get in touch with state and local responders.

The third reaction was to take a hard look at the legal infrastructure that we had in place and to do a better job of clarifying roles and responsibilities. The point was to change the law so that the government could get certain information while respecting privacy rights, before there was a "before-the-problem" and "after-the-problem" issue. The FBI needs to be able to prevent the crime a little bit sooner. Similar themes came out again in the Homeland Security dialogue.

The fourth area was kind of bizarre. It came out of one part of the White House that thought this was a White House management issue. In other words, if we looked at, in particular, the cyber problems, the conclusion we should come up with is this is just brand new information and we probably ought to fund the Office of Management and Budget to look at how we manage things in the information world.

The final recommendation was very blunt and honest. It was that we have absolutely no clue what to do; and so we are going to recommend a commission. This was very unsatisfactory. However, what they did was absolutely unique in the government's history. The recommendation was instead of having government take the lead, lets inform senior private sector leaders of everything the government knows and see what they recommend. And that is exactly what they did.

The President's commission on Critical Infrastructure Protection was well funded by the Pentagon, and in October of 1997 it published a report after a year

and a half of studying the problem. The commission essentially came up with two conclusions. The first is that we need a national risk assessment strategy and framework. In other words, it is not enough to turn to the banking community and the electrical power sector and say make your industry more secure. We need to do a better job of clarifying what they must secure against. How do we make ourselves more secure? What is the philosophy? Who pays for it? How do we address questions of liability to enable industry to complete its work without being afraid of future lawsuits?

The second conclusion was that law and policy are leagues behind in technology, and need to be closer together. The President's commission report had seventy-four recommendations. If you want to see what they look like in five pages, they were wrapped into Presidential Decision Directive 63, which was issued in May 1998. Presidential Decision Directives ("PDDs") are funny things. As a lawyer in Washington focusing only on administrative law, I had never heard of a PDD before. It turns out they are all classified. Every once in a while, the National Security Council, which writes these directives, will issue a white paper laying out what it did but keeping them very quiet. What PDDs say is that the United States is going to move forward with a complex national security issue, and that all agencies are going to march to the same beat. Clinton signed it and then issued orders to the CIA, Energy Department and OMB. It was an interesting approach to spend two to three years looking at a problem, conferring with senior private sector leaders, being very honest about what the problems were, listening to what they had to say, and then incorporating them into a White House document that said lets move forward in this direction with the President's backing.

Well, that is the good news. The bad news, of course, is that President Clinton was well known for being a bit confused. I do not mean that in a bad sense. Presidents have a lot on their minds. When the President ordered the Administration to move forward on one beat, various problems emerged. Eventually there were four or five different Presidential level processes all moving forward on the same beat, but each was competing for money, accountability, interest, and press. That is how things went until Y2K came along.

Y2K was an important turning point in terms of going one step forward and two steps back. The debate leading up to Y2K within the government was as follows. There is this glitch out there. It is very cyber oriented, and the critical infrastructure community has pointed out cyber-related problems that we need to pay attention to. One part said, we need to be really afraid of this. That part said, lets build a national risk assessment war room. Let us get the CEO's on board, let us get Congress to change the law with regard to liability, anti-trust, and freedom of information. Let us get some government funding behind it, get some accountability with the agencies. Thirty-five million dollars later, we had the very first war room ever for the national public and private sectors.

The other part of government and industry suggested that this was similar to a lot of other problems out there. In terms of the war room, a phone, a fax, a "few

good men," is really what is needed. Issues of liability are really a big fight between the trial lawyers and a bunch of other people. We ought not change competition policy and anti-trust policy just because of this glitch.

The first camp won out until January 15, 2000, when the President dismantled the war room and managed to take the whole process a step backward. We had moved forward all the way to T and then marched back to Q because we said this was a serious problem, we treated it like a serious problem but guess what? It was not that serious after all.

That takes us all the way through September 11th when the President issued two Executive Orders in October. The first forming the Office of Homeland Security and the second, forming the Office of Cyberspace Security.

In conclusion, there is a problem out there. I do not know what it is, I do not know how to govern it, I cannot even define it, and it causes me to get confused and just fall apart and feel helpless every time I spend a day talking about it. What I can tell you is we need to let this problem percolate at the highest levels of our government until we get a better handle on it. And, that is what the two Executive Orders basically do. They set up committees and processes to get a hold of some of these problems. They begin to look at things like information dissemination, public/private partnership, research and development, real funding, real accountability, and then shoot that information down into the agencies to come up with a solution.

I think we get to the letter T when we form a new department, which is decidedly intelligence oriented and which begins to look like just one of those pieces of the initial Critical Infrastructure Working Group. In other words, there needs to be more intelligence information, more "stuff 'em and cuff 'em" and then we can begin to solve this problem. Thank you.