National Security Cyberspace Institute NSCI

CyberPro

May 2010

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Jeffrey Addicott

NSCI's Lindsay Trimble recently had the opportunity to interview Jeffrey Addicott, distinguished professor of law and director of the Center for Terrorism Law at St. Mary's University School of Law in San Antonio, Texas. An active duty Army officer in the Judge Advocate General's Corps for 20 years, Addicott spent a quarter of his career as a senior legal advisor to the U.S. Army's Special Forces. As an internationally recognized authority on national security law, terrorism law and human rights law, Addicott lectures in professional and academic organizations; contributes to national and international news shows; and is the author of more than 20 books, articles and monographs on a variety of legal topics. His most recent book (2009) is "Terrorism Law: Cases, Materials, Comments, 5th edition."

NSCI: Would you please give us a brief overview of the Center for Terrorism Law?

ADDICOTT: Founded in 2003 at St. Mary's University School of Law, San Antonio, Texas, the Center for Terrorism Law is a nonpartisan, nonprofit institution [501 (C) (3)] dedicated to the study of legal issues associated with antiterrorism and counterterrorism. Particular emphasis is given to cyberterrorism, bioterrorism, critical infrastructure and information assurance technologies.

The goal of the center is to examine current and potential legal issues related to terrorism in light of the challenge of achieving and maintaining a proper balance between national security and civil liberties. As a fully operational research facility, this goal is pursued through teaching terrorism law courses, professional exchanges such as symposia and consultations; writing; commenting on and publishing written materials; conducting training; and ensuring access to extensive information resources regarding terrorism.

NSCI: How is the Center for Terrorism Law incorporating cyber issues into its research and curriculum?

ADDICOTT: Since our center is non-profit, we operate on grants and donations. As such, we will go in the direction of whatever grant money we get to study certain issues. In the past, for example, we got some grant money to study IP traceback technology and the legal issues associated with that, so we produced some whitepapers on that topic.

My concern is cyber because I think we're going to have a 9/11 cyber event in this country and it's going to be devastating. I want to start thinking about that now, leaning forward in the saddle to tackle some of the legal and policy issues to make the country safer. With that said, we're still driven by funding concerns. We are very pleased to see the 24th Air Force Cyber Command here in San Antonio. We are working with them very closely and I do all the work with them pro bono.

We also host many conferences focusing on cyber. Since the center was founded in 2003, more than half of all of the conferences we've done have been on cyber issues. Last year we did one conference in

Houston on cyber in the business sector. In March, we hosted one in San Antonio on the legal issues of cyber.

We’re not here to make money, but we’re trying to get interest. In a lot of the studies and work done in cyber, if you ask “Did you think about the legal piece of that?,” they respond “Huh, what?” Many people don’t think about the legal part and you do that at your own peril. Everything has a legal dimension and cyber has a lot of legal dimensions. We’re trying to offer that and find people that will support us with seed money to study many of the legal issues that are popping up – cyber as an act of war, what are the issues related to cybersecurity, privacy issues related to cyber. Many other universities have the funding to study cyber issues, but they don’t have a legal dimension to them. We’re trying to find the means to supply that specific piece of this very important pie.

NSCI: How would you describe the difference between cyber attacks and cyber espionage?

ADDICOTT: The term cyber security covers both concepts. While a cyber attack refers to the intentional disruption of an information system’s confidentiality, integrity or availability (CIA) (note that most disruptions of information systems are caused by unintentional human error and are called cyber incidents), cyber espionage refers to the gathering of intelligence – either in the private sector or the government sector - for untoward purposes.

NSCI: Defending against the threat of future cyber wars and large-scale cyber attacks is a hot topic for security experts. What positive steps have you seen the current administration take to secure cyberspace and protect our critical infrastructure from these threats?

ADDICOTT: From the Clinton Administration to the Obama Administration, the government’s approach to cybersecurity for owners/operators of private computer systems has been one of cooperative engagement and not mandatory regulation. Among other considerations, the general feeling was that since the civilian sector invented cyberspace, cyber security programs and processes should be left to market forces.

In short, despite the rapidly expanding reliance on the Internet by American businesses, consumers and government agencies, the government provides extremely little affirmative regulatory laws in terms of cybersecurity functions for non-government computer systems. Instead, the concept of engagement stresses the promotion of voluntary public-private alliances to combat cyber attacks of all kinds with particular emphasis on protecting the nation’s critical infrastructure. With but minor exceptions, aimed at government computer systems, the theme of engagement predominates all of the federal laws, executive orders and presidential directives associated with cyberspace.

NSCI: How do you think the creation of a “national cyber czar” will impact cyber policy and action?

ADDICOTT: I’m not very hopeful. The real thrust has to come from Congress. Congress is currently debating new cyber legislation to establish specific cybersecurity standards for various sectors in industry, but they haven’t been able to produce anything yet. This is mainly because private industry doesn't like big government; they do not believe the government can really play an important and supportive role. They also see that cyber is changing so fast that any standards that are established will be obsolete by the time you try to implement them. Also, free enterprise simply does not want the government involved in their business, so you have that tension between free enterprise and government regulation.

Once we have a cyber 9/11 event, the government – as they did with the Patriot Act – will overreact and produce Draconian cyber security standards. It's better to do it now. The government needs to work with private industry and find a road in the middle between an engagement strategy and a mandatory regulation strategy. We need to find a middle ground, where you move towards private industry and different sectors to agree that we need to have a uniform standard of cybersecurity for everybody, so we can protect the infrastructure. The current infrastructure is extremely vulnerable. Many of these companies have their own private security standards and processes. Some of them are extremely weak; some of them are connected to the Internet and are vulnerable to attack. That's the dilemma. Unfortunately, I don't see anything really happening because human nature, such as it is, we don't do anything until we have an emergency.

That's what I'm trying to do. Before 9/11, I wrote a chapter in a book published by the U.S. Army War College in 2000, predicting al-Qa'eda was going to attack us. I even put it in bold print to make it clear. Unfortunately, we need leadership at the top. The Obama administration and the cyber czar need to push as hard as they can to provide that leadership, but I don't see that coming.

NSCI: Should a more definitive cyber policy precede the passing of significant cyber legislation?

ADDICOTT: As I said before, we need an enlightened approach to cyber security that strengthens the relationship between the federal government and the private sector in meaningful and concrete methods without evolving into a federal "big brother" program that stifles private industry. This has always been the bottom line solution and one that everyone recognizes. As such, while we need a new federal policy that moves from the engagement theory towards mandatory regulation, the new policy of engagement/regulation must still operate in a way that "promotes" public and private sector coordination, research and preparation to repel or respond to a cyber attack on one or more of our critical infrastructures. Again, having the federal government attempt to directly regulate all aspects of cyber security in the private sector violates the free market principles which constitute the bedrock of this nation (even if one assumes that the government is competent enough to do so).

NSCI: What major cybersecurity legislation do you think is needed? How do we ensure flexibility in our legislation to accommodate the speed at which cyber threats evolve?

ADDICOTT: Any cyber security legislation must begin the journey from engagement towards regulation, what I call engagement/regulation. Partnering without controlling is in its infancy but it is imperative that a long-term legal shift occur to implement programs to ensure that private industry not only shares information but develops appropriate security systems. In addition, any legislation must address the hard fact that the rapid pace of advancements in cyber technology requires that the government expend the necessary funding to attract the brightest and the best individuals from the civilian sector to develop viable security standards that can be quickly amended to match evolving conditions.

NSCI: How do you recommend our nation improve cooperation among law enforcement, private industry and the government in cyber security?

ADDICOTT: In addition to the items I just mentioned, the government needs to specifically task federal agencies with developing critical infrastructure protection standards that are tailor-made for specific commercial enterprises associated with the critical infrastructure.

NSCI: At a recent conference, you expressed doubts about the international community's ability and willingness to establish common policy regarding terrorism, stating that we haven't even been able to agree on a definition of the term "terrorism." Can you explain why this has been such a difficult thing to accomplish?

ADDICOTT: Similar to the problem of obtaining universal agreement on defining the term “terrorism,” there is no generally accepted definition for “cyberterrorism.” All intentional attacks on a computer or computer network involve actions that are meant to disrupt, destroy or deny information. These attacks may be motivated by monetary gain, vandalism, terrorism or as acts of war. Thus, most cyber attacks may be categorized as cyber crimes, but not all cyber attacks are deemed to be an act of cyberterrorism or war. Clearly, the key difference between cyber crime and cyberterrorism is the concept of terror. If a universal definition of the term terrorism does not exist, one can at least list four key characteristics of terrorism that better reflect the nature of the activity:

1. The illegal use of violence directed at civilians to produce fear in a target group.
2. The continuing threat of additional future acts of violence.
3. A predominately political or ideological character of the unlawful act.
4. The desire to mobilize or immobilize a given target group.

Combining these four key characteristics, then Secretary General of the United Nations Kofi Annan offered a succinct 2005 definition for terrorism which was blocked by the 56 member Islamic Conference (who wanted an exception for wars of "national liberation"):

> [A]ny action constitutes terrorism if it is intended to cause death or serious bodily harm to civilians or non-combatants, with the purpose of intimidating a population or compelling a Government or an international organization to do or abstain from doing any act.

Adopting the general definitional theme of terrorism set out above, cyberterrorism is the improper use of various computing technology to engage in terrorist activity. Since the terror motivated cyber attack would most likely be against the critical infrastructure of a nation to intimidate or coerce another (usually a nation) in furtherance of specific political objectives, one commentator has defined cyberterrorism as “the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non combatant targets by sub-national groups or clandestine agents."

NSCI: Given these problems, how do you think the United States should proceed in the area of international collaboration and/or possible treaties related to cybersecurity?

ADDICOTT: The United States should continue to develop bilateral and multilateral treaties to assist in both criminalizing and cooperating on cyber security issues. There seems to be no move towards major international legislation.

NSCI: What do you think it will take for such international legislation to be developed?

ADDICOTT: A major cyber disaster event.

The last time we had any type of cyber legislation proposed was by the Russians in 1991, trying to develop cyber treaties to deal with cybersecurity. That was because they had just come out of the Cold War. They were weak and they wanted to weaken the West. But since they've become stronger, there's no concern by any country about developing any type of cyber stuff. There are various criminal statutes that we work to cooperate on bilateral arrangements, but there's nothing significant out there, in terms of international law and cyber agreements.

When one country gets hit that's a major power – not like Estonia, a tiny little country – but a big country, they'll get motivated.

NSCI: Is there anything else you'd like to add?

ADDICOTT: The primary concern is that a cyber attack will target one or more of the nation's critical infrastructures. The almost seamless interconnectivity of the Internet presents a readily available and inexpensive opportunity for computer network cyber attack. The cyber threat must be met with the same recognition and gravity as a physical terrorist attack. In order to secure the nation against cyberterrorism, security officials must not be lured into believing that terrorist organizations, such as al-Qa'eda, lack the necessary equipment and knowledge needed to implement such an attack.