LBAR Lesson IX: Security (Part 3 – Political Security)

We saw in the last lesson that, just as it is with people who make themselves targets of malicious behavior when they use Cyberspace to communicates, so too does government make itself a target when it makes use of Cyberspace to facilitate communication with American citizens. We noted that, in addition to the many threats brought to bear on individuals in Cyberspace, the United States government also faces other threats: the hostile actions of enemy states and non-state actors. Especially noteworthy today are the threats posed by terrorists; Cyberspace is just as much a tool for terrorists to communicate, organize and carry out hostile actions as it is for peaceful and law-abiding citizens to communicate on an everyday basis. This means that the United States government must protect its own information and computer systems for harm just as it is tasked with protecting American citizens from harm.

But how does it do that? How can our government protect us from those that would do us harm if those people never meet physically? Old cop shows always had what were called stake-outs, where the cops would sit in a parked car off to the side of the street, waiting and watching for criminals to happen by so they could arrest them. But crime does not work that way anymore; those who are up to no-good do not meet together literally; they can now meet "virtually" in Cyberspace, making it hard if not impossible to know what they are doing, much less catch them in the action. Yet, especially when it comes to terrorists, our government must do this. But why? Why can ordinary citizens not catch terrorists in the act?

First, it is enough to remember that, in the United States, we ask of our government that it do very specific things, and we require of it to do those things in very specific ways. The truth of this was set out long ago in the Declaration of Independence, which was a formal declaration (written by Thomas Jefferson) issued by the First Continental Congress in 1776 in Philadelphia. A declaration is a statement; it declares something of importance, in this instance it declares why these 13 former British colonies think they should be independent. In the Declaration of Independence Jefferson explains that Americans hold certain truths to be self-evident – "that all Men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the Pursuit of Happiness". We form government to secure these rights; "That to secure these Rights, Governments are instituted among Men, deriving their just Powers from the Consent of the Governed". You can see then this basic and must fundamental of American documents already articulates what we ask of our government – we want it to protect our lives, liberties and pursuit of happiness. Government thus must catch and stop criminals, but also enemies; Cyberspace merely adds another mechanism whereby enemy states can do us harm. Yet enemies are not like criminals; criminals claim the protection of the law, but deny it to others (which is why they do not want you talking their stuff, but will gladly take yours). Enemies deny the law as such; they reject American law because they reject how and why American law is made, which means they reject America as such. The threat level posed by enemies is thus different in kind that that posed by criminals; criminals steal money and damage computer infrastructure while terrorists kill people, and ultimately hope to destroy the government.

The U.S. government must then be proactive when it comes to the ways in which terrorists could make use of Cyberspace. Can you think ways in which terrorists could use Cyberspace to plot terrorism? How could every one of the social media sites you regularly use also be used by terrorists? More broadly, think of every way in which you use Cyberspace. Now, think of how terrorists could use Cyberspace in exactly the same way. Given the magnitude of all this, how can the U.S. government effectively combat terrorism? What techniques might it use to learn what terrorists are planning? Is

there anything it should not do when trying to learn about terrorists? If not, why not?