

Terrorism Redefined?

By

Lt. John Dewar
Pasadena Police Department

September, 2009

COMMAND COLLEGE CLASS #45

This Command College project is a FUTURES study of a particular emerging issue in law enforcement. Its purpose is not to predict the future, but rather to project a number of possible scenarios for strategic planning considerations.

Defining the future differs from analyzing the past because the future has not yet happened. In this project, useful alternatives have been formulated systematically so that the planner can respond to a range of possible future environments.

Managing the future means influencing the future, creating it, constraining it, adapting to it. A futures study points the way.

The view and conclusions expressed in this Command College project are those of the author and are not necessarily those of the Commission on Peace Officers Standards and Training (POST).

TERRORISM REDEFINED?

Imagine yourself and your department personnel responding to the following scenario: a car bomb detonates in the parking lot of a local high school during regular school hours. Hundreds of students are injured or dead. As your officers are racing to the scene, radio communications begin to shut down. There is nothing but static on the air. Sergeants can't communicate with officers to coordinate a response plan. Fire and paramedic personnel lose their communications as well. Officers arrive to the campus amid chaos. They drive around trying to find a command post. There is none. Communication amongst first responders can only be accomplished face-to-face; mutual aid coordination is virtually impossible. As parents learn of the attack, they converge on the school in panic.

You reach for your cell phone, punch in numbers to Dispatch. You get a busy signal.....cell phone service is down, too. At the same time, Dispatch sees its 911 system shut down. People calling into the station get a busy signal. Verizon Wireless notifies Dispatch via landline that their system has just crashed over an entire region; a computer overload of some type. Your City Public Works dispatcher notifies your communications personnel there are disruptions in the electricity grids in the region. Water and power systems are also failing. Street lights at intersections are out. Regions of businesses and homes are temporarily without power.

Your regional Emergency Operations Bureau command center struggles to regain communication. EOB personnel soon understand what first responders quickly found out: that the terrorist bombing at the high school had been accompanied by a simultaneous cyber attack against the region's electronic, power and communications systems.

A frightening scenario? Yes. Could it occur? Yes; today.

This scenario describes the multiplier effect that a combined cyber/physical attack would have on a police agency and the surrounding region. And it begs the question: How prepared is your department to respond to a critical incident during which your communications and computer systems are under simultaneous cyber attack?

Attacking the Grids

On December 27, 2001 Osama bin Laden stated the following in a video released to the world: *“It is very important to concentrate on hitting the U.S. economy through all possible means.....look for the key pillars of the U.S. economy. The key pillars of the enemy should be struck.....”* (Bin Laden, Osama, “Messages to the World”, 2005)

Cyber terrorism is defined by the FBI as any 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 (www.SearchSecurity.com, August 26, 2008). Since 9/11, law enforcement agencies have increased their focus and training to respond to potential terrorist attacks. The results of that training are evident today: officers are more knowledgeable, and they are armed with better intelligence and equipment. There is more inter-agency collaboration. The good news is we are better connected than ever.

That is also the bad news.

The Information Super Highway has become the path by which we are connected to one another throughout the world. It is a highway that allows access to anyone, friend or foe, with a laptop and an Internet connection. But this highway also leads to our most critical computer-operated infrastructures: power grids, communications, water, banking and unlimited amounts of

sensitive data. Our lives are embedded in the cyber world we created. And this presents law enforcement with a unique dilemma: The communications and computer systems we rely upon in our law enforcement agencies to respond to emergencies and make our cities safe may be looked upon by our adversaries as our Achilles Heel.

Recent Incidents

A brief review of recent cyber attacks and intrusions shows that the ability to launch cyber warfare against our critical infrastructure is real.

Prior to 9/11, law enforcement had little concern about infrastructure protection. Our power grids, water systems and communications never “appeared” to be under any credible threat. Computer “hacking” was the first evidence to the general public of any vulnerability in our computer systems, but it was a phenomenon promoted primarily by computer whizzes in college. Law enforcement agencies have become more aware of computer crimes over the recent years, although they are usually synonymous with stealing one’s identity or fraudulent use of bank accounts. It isn’t until quite recently that law enforcement agencies have taken a more serious look at their critical computer-based infrastructure as a potential target. Recent news headlines underscore that emerging threat:

- U.S. authorities concede that in the early 1990s China initiated *Shashoujian*; a military term that loosely means creating a military weapon or strategy that can get the better of a seemingly invincible enemy. The result is that the Chinese have been investing heavily in 3 weapons systems: an anti-satellite missile system to knock out our satellites, ultra-quiet diesel electric submarines, and cyber weapons

to attack our computer-based infrastructures (Wall Street Journal, April 14, 2009 A13).

- “South Korea Analyzes Hacked Computers” (USA Today, July 13, 2009, B1)
South Korean police analyzed some of the thousands of computers in South Korea and the United States attacked by a North Korean Military Internet Warfare Unit.
- “Hiroshima, 2.0” (The Wall Street Journal, April 14, 2009, A13) The U.S. government reports widespread cyber-spying of the U.S. electronic grid, much of it apparently originating in China and Russia.
- “Obama Set to Create Cyber Czar Position” (The Wall Street Journal, May 29, 2009, A4) The President moved to create a new director amid growing concerns that sophisticated attackers will wage a cyber assault on critical infrastructure networks. Russian and Chinese attackers have repeatedly penetrated U.S. electric and power grids.
- “11 Charged in Massive Identity Theft” (Menn, Joseph Los Angeles Times, 2008)
More than 40 million account numbers were stolen from computer systems. The worldwide investigation revealed the global nature of criminals using the Internet. Suspects were tracked from China, Turkey, Germany and the Ukraine. American suspects included 10 members of the local Long Beach “Insane Crips” street gang.
- “Even before Russians Troops Arrived, Georgian Government Websites were under Cyber Attack,” (Los Angeles Times, 17 August 2008, A25). Simultaneous Denial-of-Service cyber and physical attacks by Russian military forces against

Georgia in 2008 illuminated just how unprepared the world is for this new kind of warfare

- Closer to home, even the California Independent System Operator, which coordinates and monitors electrical and power systems throughout the state, acknowledged recently that our system in California is vulnerable to a cyber attack (Pasadena Star News, 2009).

These are but a few of the recent headlines that should give us in law enforcement pause in examining the extent to which we might be vulnerable from cyber attack at the local level. Clearly, if 10 local street gang members from Long Beach can steal information from computers worldwide, or a North Korean Cyber Warfare Unit can attack a power grid in Pittsburg, PA, how can we assume our local piece of the Information Super Highway is safe?

How will we be attacked?

Critical infrastructure is a “good” target for cyber terrorists because most sectors are relatively exposed, vast, interconnected and unprotected (Lewis, 62). In lay terms, a cyber attack occurs when a skilled computer user intentionally attacks a data-filled target over the Internet. There are typically two centers of electronic information that comprise the main targets in our society: data systems, and control systems. Our police departments use both.

A cyber attack is going to do one or more of the following to either target system:

- Steal data
- disrupt or damage data
- deny access to data or access to computers
- Spread disinformation

- shut down control systems

Supervisory Control and Data Acquisition systems (SCADA systems) are the standard computers and servers used in gas, water, electric and telecommunication grids across the country. They are found in almost all industrial processes (Lewis, 72). Our electronic power grids are controlled by SCADA systems which are often accessible through the Internet, DSL lines, digital radio and Wi-Fi wireless or by telephone modems. Current technology allows employees to operate these systems remotely or by dialing in with a modem. Of course, law enforcement widely uses many of the same systems, networks and technologies to conduct their business; from sharing criminal data information, storing documents and public records, and even to perform the daily activities endemic to any organization.

One might think that systems can be isolated and protected easily, but that often is not the case. Network systems, in reality, are typically interconnected with corporate networks, business partners, websites, and databases outside of law enforcement. There are so many “walls” that can be breached from different access points. If employees can access these systems that control our infrastructure, so can attackers. A primary means of attack might be to breach security, and then manipulate or share the data resident therein.

Another method of attack is the Denial of Service (DOS) in which attackers “hijack” thousands or millions of other computers which then saturate a computer system with requests essentially shutting down the computer operation. This forces the operators to reroute their entire network to new servers which, depending on the size and complexity of the systems, could take hours or days to accomplish.

The danger of these types of attack occurring will only increase as our young computer-savvy generations around the world come of age. And the vast number of potential targets

guarantees that terrorists will be able to locate weak points to attack in unconventional, asymmetric ways.

Terrorists think asymmetrically

Cyber warfare may be appealing to terrorists for several good reasons: it is certainly inexpensive since an attacker needs only a laptop and an Internet connection. It is also an anonymous method of attack, since attackers can “hide” in the Internet and can attack from remote locations. National War College military theorist Lt. Colonel Kenneth McKenzie defined asymmetric warfare in 2001 as “Leveraging inferior tactical or operational strength against American vulnerabilities to achieve disproportionate effect with the aim of undermining American will in order to achieve the asymmetric actor’s strategic objectives” (Asymmetric Warfare, Lt. Colonel McKenzie, 2001, www.iwar.org). Terrorists seek ways to make up for their inferior power by striking at critical, poorly-defended targets. Their goal is to sow terror in the hearts of our people and cripple our economy. Their ability to merely disrupt our basic human desire to stay connected might be all that is needed to accomplish their goal. Doing so through inexpensive and achievable disruption to our core electronic systems may be one the best ways to accomplish this task.

One should not assume that attacks will be lead by uneducated assailants. Many of the recent terrorists arrested in Europe and Great Britain are well-educated. Government officials recently uncovered several on-line Internet Jihadist forums, hosted in Europe, where advanced instructions were given for computer hacking (Baldor, Lolita, San Gabriel Valley News, 2009). Computer experts, including those capable of breaching government infrastructure, were being sought for the jihad. Americans have always fought the enemy in some other part of the world.

We have become accustomed to being able to confront our adversary far away and defeat him on the battlefield. That is not the case if the method of warfare utilized is the Internet: the enemy is capable of being right here with us.

How vulnerable are we?

Try to imagine any activity within your police department that does not involve computers or the Internet. Extend that line of thought to your department: your patrol units and command post, for example, are crammed with electronic gear, laptops, and in-car video. Now extend that further to your First Responders arriving to a critical incident and all their means of communicating crashes. Lastly, add the multiplier effect of thousands or millions of people in your region who are directly affected by the cyber attack. This is exactly what a simultaneous cyber/physical attack is about: shutting down those critical systems thereby crippling police response and simultaneously instilling panic in the population.

How vulnerable is your city? Take a moment to scan your city's infrastructure. Are your power, electric and communication stations well-protected? Do you know where they are? Has anyone from your police agency worked with your Public Works and IT staff to assess vulnerability? Are there back-up systems; if so, what are they? More importantly for you, which of these systems, such as radio communications and computers, are tied to your first response capacity? How safe are they from cyber intrusion?

The federal government has issued a directive of what is considered to be the Critical Infrastructure Sectors of our society: the most likely targets of terrorist attack (Lewis, 38). Included amongst the 13 sectors noted is the Technological/Communications infrastructure. Given that almost all of the listed sectors (public health, energy, defense, shipping and

emergency services, etc.) rely on networked technologies, a cyber attack may be the most proficient means to destroy the most critical components of our society.

Assumptions

As law enforcement officers we must not assume that other city employees or departments are managing cyber security or our ability to respond under such an attack.

Let's look at some assumptions your department may be making related to a terrorist attack:

- The attack will be only physical in nature (no punctuation in a list)
- The attackers will be at or near the scene and eventually isolated and dealt with by First Responders
- Command posts will operate with the use of communication technology and computers, cell phones etc and there will be mutual aid coordination with other agencies
- Outside of the critical incident scene, the rest of the city or region will likely not be directly affected

Do your First Responder training plans mirror these assumptions? What if your assumptions are incorrect and the "site" of attack is actually via the Internet? And the attackers are "there" but not really. Do you have a plan to adapt to that change?

What Needs to Be Done?

We know that our society is vulnerable to a cyber attack. And we know that a well-timed combined cyber/physical attack would strain available resources beyond our limits. What kind of steps can we take now, and into the future, to mitigate such an attack, and to respond and manage the incident effectively if one does occur?

- The chief or sheriff must communicate that cyber security is a top priority in emergency planning. The level of commitment displayed by the boss will, in great part, determine the success of the project and of any associated funding
- Determine which infrastructure nodes in your city are the most vulnerable. This will require a partnership with Public Works, IT and private sector businesses
- Prioritize the list. This will assist in the proper allocation of resources and funding to the most critical locations first
- Develop a timeline for implementation to protect these key sites
- Establish a working group of police, IT, Communications and Public Works experts to determine which infrastructures support First Responders. This includes radio frequencies, computer systems, wireless technology and power systems
- Ensure that only trusted, key people have access to the critical infrastructure that supports emergency operations. Never assume employees are not vulnerable to influence or corruption. Passwords must be verified and changed often
- Ensure that redundant, back-up communications systems are in place that can function in the field for First Responders when all other systems fail. If there is none, create one. This may be something as simple as direct-talk, walkie-talkies

- Test these redundant back-up systems in real-time training scenarios. Include these tests in regional, mutual aid training days. Include mock cyber attacks into the training matrix
- **If you do none of the above, at least do the following**: suggest that during your department's next critical incident training day, a decision is made to shut down all communications, power and computer systems during the exercise. See how quickly your First Responders can flex to the change, if at all. It should be immediately clear if your department is prepared to handle a cyber attack during a real critical incident

Conclusion

Imagine now a more positive ending to our opening scenario: your First Responders are racing to the site of the bombing. Dispatch advises that some type of cyber intrusion has occurred in the local communications and power grids, but attackers have not gained access past network defenses. Patrol supervision nevertheless orders all responding personnel to switch to direct-talk radios. Back-up communications and power systems, separate from computer-aided dispatch and the Internet, switch on automatically. First Responders, now using a secure communications system, assume control of the incident to its conclusion. The simultaneous cyber attack has been thwarted. A plausible scenario? Yes, and it is possible today.

Law enforcement has the core responsibility to provide for the safety and security of our communities. We must be knowledgeable about the rapidly changing environment and adapt our organizations to meet these challenges. One such challenge is the use of the Internet by terrorists to further their goals of creating chaos and terror in our communities. This is a significant challenge to law enforcement now and will be more so in the years to come. We must also be clear about our vulnerabilities. Our profession demands that we succeed in worst-case scenarios.

A combined cyber/physical attack is such a scenario, one against which we must train and for which we must integrate countermeasures.

We are all connected to the Information Super Highway. Those police agencies that understand this connectivity and its potential for harm to come our way will be in the best position to safeguard against it. If they don't, those who would see a disruption to our critical infrastructure as a good thing have a clear path to success.

References

Asymmetric Warfare, Lt. Colonel McKenzie, 2001, www.iwar.org

Baldor, Lolita, San Gabriel Valley News, Officials: "Militants exploiting Internet" A9, June 19, 2009

Bin Laden, Osama, "Messages to the World (Speech for 19 students)" Bruce Lawrence (Editor), Verso Publishing, 2005

Department of Homeland Security, "Cyber Storm Exercise Fact Sheet, (30 August 2008)
<http://dhs.gov/xnews/releases>

Hoffman, Stefanie, CRN (12 August 2008,) "Russian Cyber Attacks shut down Georgian Websites" <http://www.crn.com/security>

Joseph Menn, Los Angeles Times, "11 Charged in Massive Identity Theft," Los Angeles Times, 6 August 2008, A1

Lewis, T. Critical Infrastructure Protection in Homeland Security, (John Wiley and Sons, Inc 2006)

Pasadena Star News (April 9, 2009) "Nation's Electric Grid Target of Hackers," A1

Search Security (2008, August 26) What is Cyber Terrorism?
<http://searchsecurity.techtarget.com/definitions>

The Wall Street Journal (May 29, 2009), "Obama set to Create Cyber Czar Position", A4,
www.thewallstreetjournal.com

The Wall Street Journal (April 14, 2009), Hiroshima, 2.0, A13, www.thewallstreetjournal.com

USA Today (July 13, 2009), South Korea Analyzes Hacked Computers, B1, www.usatoday.com

Verton, Dan. Black Ice: The Invisible Threat of Cyber-Terrorism, (McGraw-Hill Professional, 2003)