To: Richard Durbin, United States Senator (IL)  
From: Andrew Schleicher  
Re: International and Domestic Rail Security Challenges and Future Trends  
April 1st, 2010  
-----------------------------------------------------------------------------------------------------------------------------------------

Senator Durbin – per your request, and in light of the recent attacks against the Lubyanka and Park Kultyty stations in Moscow, I’ve analyzed and identified future trends and methods available to security experts to secure U.S. rail systems. Hopefully, this primer will be helpful as grounding for possible policy changes or additions.

Understanding the challenges of securing the rail systems requires in-depth analysis of structural and historical weaknesses in transportation security infrastructure. Rail mass transit is, by design, a system based on quick, anonymous access and exit. Historical physical counterterrorism measures have done little to prevent dedicated adversaries in carrying out attacks. In fact, more often than not attacks are thwarted not by security countermeasures, but by carelessness or failure of adversaries to plan and execute attacks properly. The fact that rail terrorism occupies a small and distant portion of the security infrastructure of our nation is not grounded in the likelihood or possible damage in an attack, but a fundamental lack of options. There simply is no good way to secure rail systems. With this in mind, expect rail transit attacks to maintain or increase their frequency in next decade, and anticipate more attempted attacks in the United States on railway systems.

Structural Risks Involved in Rail Mass Transit

Understanding why rail systems are a security nightmare is simple; what makes a metro system flow effectively for commuters makes creating countermeasures incredibly difficult for security experts. Train schedules remove unpredictability – one of the only natural defenses that targets have against attack. The quick ‘on-off’ method that keeps commuters on time to their destinations also helps attackers enter and exit an attack grid unchecked. Commonly, commuters carry bags, briefcases and airplane luggage onto metro systems, making ‘suspicious cargo’ a norm, not an exception. Tourists often make use of mass transit, decreasing the possibility of utilizing community knowledge to spot strangers. Efforts by civilians to detect and identify suspicious behavior or individuals are curtailed by the amount of strange activity that inevitably occurs on rail systems.

Expect usage of mass transit to increase – an increase in urban populations over the next several decades will make it more economically feasible to use rail transit for work than personal vehicles. Additionally, with a questionable energy future around the world, the appeal of low energy, low environmental travel impact will appeal to common travelers, both locals and tourists. Increased connection to central hubs will make trains run near, beneath and over other high-value targets. Funding for such expansion will be generated by private and semi-public sources, which will leave little funding or interest in security measures. Since rail systems often travel across county, state and even country lines, developing jurisdictional responsibility is also a major challenge.

Combined, this presents a serious challenge for security personnel and counterterrorism efforts. From a red-teaming perspective, all the potential markers for a successful attack exist. Targeting trains for attacks using Improvised Explosive Devices (IEDs) or medium sized Vehicle Borne IEDs (VBIEDs) is relatively simple and inexpensive. Future centralization of mass-transit will increase the economic and symbolic damage done by an attack (this paper does not attempt to address the economic vulnerabilities and weaknesses of shipping or cargo transit, which is, in a word, great). Coupled with the poor security systems in place and the good possibility of initial escape from the scene, adversaries place rail systems high on the list of target priorities. Planning and reconnaissance is much easier when terrorists role-play as tourists, snapping pictures and filming both targets and security under guise of visiting guests. Practice attempts can be carried out as simply as using the rail systems.

Historical attacks inside the U.S. & Abroad

With all the vulnerabilities that rail systems possess, it comes as no surprise that the world has seen an incredible influx of high profile rail attacks since 9/11 and the world’s increased focus on terrorism. Below is a selection of noteworthy, high profile attacks.

**Moscow [04]:** Chechen rebels conducted an attack on Zamoskvoretskaya Line killed 50 and wounded 100. The attack was a part of a series of attacks dating back for a year, involving “ineffective” (low casualty) IED strikes against buses. It appeared that the terrorists used explosive vests in the attack.

**Madrid [04]:** The Madrid train bombings have been described by many as Europe’s 9/11. Four trains were targeted in the Madrid attack, which killed 191 and wounded 1,856. The first train was rocked by explosions at 6:37am, and two minutes later, three other trains had been ripped apart by explosions on the rail system. The bombs utilized 22 pounds of explosive material, and 2.2 pounds of shrapnel designed to increase casualty numbers. In all, 10 bombs were detonated, while three failed to detonate.

**London [05]:** Three explosions took place in the rush hour traffic of metro London’s Underground metro system, causing 52 fatalities and over 700 injuries. A fourth explosion on a double-decker bus brought the transportation system of downtown London to a halt. Again, IEDs were used, comprised mainly of organic peroxide.

**Delhi [06]:** The Suburban Railway system of Mumbai was hit by a series of explosions during the evening rush hour, killing over 200 and wounding 700 more. Seven pressure cookers were used as IEDs in the attack, designed with RDX and ammonium nitrate.

**India/Pakistan [07]:** An express train between Delhi and Lahore was hit by IEDs during the midnight hour, killing 68 and wounding 50 more. The IEDs, briefcases in this attack, were filled with kerosene, and many experts inferred that the weapons were expected to kill as incendiary devices, rather than explosive devices.

**U.S. [Attempt Unsuccessful] [09]:** An attempt against the New York City Subway system by NajibullahZazi involved 3 backpack bombs, to be detonated in the Times Square and Grand Central Stations. The devices, which were never constructed, were apparently of hydrogen peroxide design.

**Moscow[10]:** Again, Chechen rebels attacked the Russian Metro system, killing 40 and injuring 100. Again, suicide bombs were created for the attack, created by mixing RDX and TNT and detonated most likely via mobile phone.

The short list of high-profile attacks here yields an instructional set of findings.

* While motives are varied, methods are consistent. Chechen terrorists use suicide bombers (increasingly female) and are motivated by a separatist agenda. Lashkar E-Taiba, responsible for the ‘06 Mumbai bombings, utilized fairly standard IEDs, and is motivated by a radical Islamist agenda. Destabilization of international relations, the result of the firebombing attack on the rail system between India and Pakistan, is a motivation, but whose motivation it was is still unclear. Despite these varying attack motivations, each of these attacks shares a standard attack profile, of IEDs or suicide IEDs delivered on a train in motion or at a station where a train is approaching or loading/unloading passengers. Additionally, most of the attacks were staged or planned during rush hour to inflict maximum casualties.
* Fatalities and casualties are similar and minimal. Despite the vulnerabilities of rail systems, the amount of maximum damage done in terms of human life lost is relatively minimal. Though the Madrid attacks are labeled as the “9/11 of Europe”, less than 200 people were killed. In fact, no other attack comes close to the fatality numbers in the 9/11 attacks. In spite of the media coverage, these attacks are relatively small.
* Materials for attack are readily available in many countries, excluding the United States. The material for the attacks, specifically the explosive material in the IEDs, is readily available in most countries, and can be acquired with little suspicion. RDX and TNT are poorly safeguarded in developing countries, where military control on supplies is sometimes minimal or corrupt. Ammonium Nitrate is available via the purchase of some fertilizers, which is normally ordered in bulk in legitimate purchase. Organic peroxides, specifically acetone peroxide, can be easily created with requisitioned materials and has become a semi-standard component of IEDs in some organizations.

Counterterrorism in Context – Rail System Security

Counterterrorism methods can take many forms. For this discussion, the roles of Active CT (counterterrorism operations undertaken by security institutions, police forces and intelligence analysis), and Passive CT (physical security measures, technology, screening and monitoring systems) are most applicable. In a historical context, development of rail security is relatively new. Aviation security existed in the ‘security conscience’ since the ‘60s and ‘70s, when a rash of hijackings took place across the globe. Even with this 40 year legacy of development, security systems were still not strong enough to prevent the attacks of 9/11. Rail security has no such lengthy history, and experts are at a disadvantage creating many of these programs in a learning environment.

****Active Counterterrorism [A-CT]****

Rail systems have an abundance of A-CT methods to counter attack scenarios. Common countermeasures in rail systems include police searches, bomb-sniffing dogs and scanning equipment in random patrols. These methods adhere to the conventional wisdom that adversaries will see the possibility of search and seizure of personnel and equipment by security operatives, and be deterred. This unpredictability of CT operations increases the risk associated with the attack scenario most commonly used in rail attacks, and acts as a deterrent. In the United States, these A-CT operations are in place in many high profile rail systems, including New York, Washington D.C. and Chicago mass-transit lines. Programs like ‘Blue Tide’ (Terrorism Identification and Deterrence Effort) look to present “major, high-visibility, anti-terrorism show[s] of force.” The success of such programs is difficult to analyze. Random searches and bomb-sniffing dogs represent another portion of the CT toolkit in rail security. Following the 2010 Moscow attacks, train systems across the globe increased A-CT methods by increasing random searches and deploying more identification and detection crews.

Passive Counterterrorism [P-CT]

Unlike A-CT, passive counterterrorism methods are much less utilized in rail security. Recently, many rail systems have begun installing CC-TV cameras in stations and train cars. Before the past decade, however, cameras were the exception, not the rule. Additional P-CT measures, like metal detectors, x-ray scanners, and ‘sniffing’ machines are in little to no use in rail stations around the world. However, these efforts are on the rise, and in at least one case (India/Pakistan ‘07), the installation of metal detectors was a direct result of the attack.

A-CT and P-CT come from two different schools on stopping attacks – A-CT goes a long way in attempting to stop attack scenarios during and before attacks. P-CT approaches counterterrorism in a different way – it attempts to diminish attack strength and physical vulnerability, thus making rail terminals and trains less appealing targets. In this school of thought, CC-TV cameras are less for stopping an attack in progress (though they can still be used in such a way if diligently monitored) and more for post-attack analysis. If adversaries lose the ability to escape and re-plan attacks (assuming a competent police force can track down attackers), then the attack scenario may become less attractive. Similarly, physical hardening of trash bins, the architectural redesign or modification of stations and train layouts all move towards creating less “central” stations, and decentralizing targeted civilians.

Future Counterterrorism Options

Counterterrorism methods today revolve around the use of P-CT and A-CT methods to dissuade attackers from hitting rail targets. It’s likely that the future holds a mix of A-CT and P-CT methods to increase security on rail systems, but not fundamentally alter how defenses are established. What might some of these systems look like? Expect private and government sources to address the key vulnerabilities of mass-transit systems, attempting to turn them into strengths. Some defensive possibilities may not require vast technology improvements, but changes in methodology or culture.

Dual use programs seem a likely candidate for further development in the future. These programs would address P-CT necessity and at the same time integrate themselves into the everyday usage of rail transit. For example, turnstiles are currently being designed that not only accept and scan payment methods, but also actively scan for chemical and explosive trace residues. If residue is detected, the turnstile system would lock down, barring entry onto a train or platform, and inform the proper authorities. This P-CT measure would reduce structural vulnerability of easy access, as current rail systems already utilize this system, but don’t use it as a security measure, rather as payment methodology. Incorporating a dual use system could not only deter attackers from making an attempt, but could also halt or hinder an attempt at the execution phase of the attack. Making these programs effective represents its own set of challenges, however. Dual use programs would have to streamline, rather than hinder, travel speeds in mass transit. Additionally, marketing these programs to privately or quasi-publicly held transit firms may be difficult. If dual use programs can be executed that not only effectively increase security, but also streamline and increase efficiency, they could be a powerful tool to add into security systems on rail systems.

Another weakness that should be addressed is the predictability of rail systems. While nothing can feasibly be done about that predictability, the security systems at stations and on trains should be anything but. Unpredictability is one of the strongest weapons wielded against possible attacks. Shifting defensive profiles make planning and preparatory attempts less reliable, and can thwart attacks before or during the execution phase. A simple and effective change to the current security apparatus could be to rotate and modify P-CT and A-CT measures to present a shifting front for adversaries. In one specific timeframe, bomb-sniffing dogs and heavy patrols would set a level of defense that adversaries would be forced to address. At a scheduled “shift-change”, these patrols could dissipate, and random bag searches and undercover operatives could be established. Changing defense styles, intensity, and frequency could add additional levels of unpredictability in defenses.

Behavioral profiling could decrease the freedom of action that adversaries thrive on in rail attacks. By training and indentifying security teams on the indicators of suspicious behavior, the effectiveness of police presence would increase dramatically. Behavioral profiling, a system currently in place at Israeli airports, is designed around recognizing indicators of terrorist behavior. This includes clothing anomalies, physical signs of nervousness, discomfort or fear, and other factors. While a certain amount of behavior profiling falls under “good police-work”, embracing a rigorous training program with comprehensive indicator training would be a good investment for any police force, and would teach a valuable skill for any security environment, not just rail security.

Establishing a culture of security within our rail systems, in its truest form, would mean counterterrorism existing as a normal, background environment. Some aviation P-CT has already made this conversion, where it is standard procedure to move through security at airports. Despite the constant underlying grumblings from the public, screening checkpoints patrolled by TSA officers drastically increase security and have become a part of every traveler’s journey. While the robust defense existing at airports is unlikely to be replicated on mass-transit, some level of screening and security measures could make its way onto stations in a fashion more structured than previously considered. Adding to this culture must be the awareness of the public, whom security experts rely more and more to report suspicious behavior or objects in today’s mass-transit environment. PSAs promoting citizen awareness are in place in many rail systems.

Likelihood of attack – abroad and U.S.

The likelihood of terrorist attacks on rail systems is fairly certain. Assuming terrorism continues to be an effective tactic in asymmetrical warfare and continues to effect and change policies of those in power, you can expect rail systems to be high on the target lists of those engaging in terrorism. Addressing the structural vulnerabilities of rail systems is oxymoronic, and while security apparatus can work within the current environment to strengthen defense methods, it’s unlikely the fundamental challenges can be addressed in the next decade or two.

With this environment understood, recognize that despite all their vulnerabilities, the U.S. has yet to be the target of a highly successful rail terror attack. Reasons for this are unclear. Amongst academic literature, which tends to over-predict terror attacks, experts suspect the difficulty of obtaining materials, training and technical know-how without the intelligence community catching wind of danger leads to the lack of attack successes. Additionally, others have indicated that, despite the holes, the aviation “no-fly” list has done an adequate job of keeping those with the ability to perpetrate these attacks off U.S. soil. Personally, I feel our intelligence community has superior methods in place to detect attack preparation behavior, and heads off adversaries before the attack execution phase.

In countries where military and industrial supplies are more readily available (legally or illegally), and security communities are less robust, you can expect sustained or increased rail attacks. In a targeted sense, it seems that Chechen rebels have found a niche in targeting Moscow with a variety of mass-transit attacks. In a country which colloquially has a “spring terrorist season”, it would be expected that Russia lead the way in attempting to secure rail transit from attackers. Yet Moscow’s main threat, that of separatists from Chechnya and Dagestan, has been met more with A-CT and offensive action by the FSB (looking to cut off the head of the dragon) rather than defensive P-CT measures.

The sophistication of future attacks is unlikely to increase. Part of the appeal of rail system attacks is the relative simplicity of the attack profile, and changes to that profile to increase damage or casualties would likely require large increases in the technological capabilities of adversary organizers.

Conclusion

As with many other terrorist threats, it is unlikely that the funding, effort and will for action will exist before a major attack is successful. That unfortunate reality is slowly changing, but not quickly enough for the threats that are currently facing the United States. The rail security threat should be a pressing concern, and the information currently available shows no sign that the threat is subsiding. If any change can be expected, the threat of terror attacks on subway and rail systems will be increasing in the next ten years, and security systems should be updating, modifying and strengthening countermeasures in response.