The Coming Urban Terror

Systems disruption, networked gangs, and bioweapons

by John Robb

Originally published City Journal, Summer 2007

For the first time in history, announced researchers this May, a majority of the world's population is living in urban environments. Cities—efficient hubs connecting international flows of people, energy, communications, and capital—are thriving in our global economy as never before. However, the same factors that make cities hubs of globalization also make them vulnerable to small-group terror and violence.

Over the last few years, small groups' ability to conduct terrorism has shown radical improvements in productivity—their capacity to inflict economic, physical, and moral damage. These groups, motivated by everything from gang membership to religious extremism, have taken advantage of easy access to our global superinfrastructure, revenues from growing illicit commercial flows, and ubiquitously available new technologies to cross the threshold necessary to become terrible threats. September 11, 2001, marked their arrival at that threshold.

Unfortunately, the improvements in lethality that we have already seen are just the beginning. The arc of productivity growth that lets small groups terrorize at ever-higher levels of death and disruption stretches as far as the eye can see. Eventually, one man may even be able to wield the destructive power that only nation-states possess today. It is a perverse twist of history that this new threat arrives at the same moment that wars between states are receding into the past. Thanks to global interdependence, state-against-state warfare is far less likely than it used to be, and viable only against disconnected or powerless states. But the underlying processes of globalization have made us exceedingly vulnerable to nonstate enemies. The mechanisms of power and control that states once exerted will continue to weaken as global interconnectivity increases. Small groups of terrorists can already attack deep within any state, riding on the highways of interconnectivity, unconcerned about our porous borders and our nation-state militaries. These terrorists' likeliest point of origin, and their likeliest destination, is the city.

Cities played a vital defensive role in the last major evolution of conventional state-versus-state warfare. Between the world wars, the refinement of technologies—particularly the combustion engine, when combined with armor—made it possible for armies to move at much higher speeds than in the past, so new methods of warfare emphasized armored motorized maneuver as a way to pierce the opposition's solid defensive lines and range deep into soft, undefended rear areas. These incursions, the armored thrusts of *blitzkrieg*, turned an army's size against itself: even the smallest armored vanguard could easily disrupt the supply of ammunition, fuel, and rations necessary to maintain the huge armies of the twentieth century in the field.

To defend against these thrusts, the theoretician J. F. C. Fuller wrote in the 1930s, cities could be used as anchor or pivot points to engage armored forces in attacks on static positions, bogging down the offensive. Tanks couldn't move quickly through cities, and if they bypassed them and struck too deeply into enemy territory, their supply lines—in particular, of the gasoline they drank greedily—would become vulnerable. The city, Fuller anticipated, could serve as a vast fortress, requiring the fast new armor to revert to the ancient tactic of the siege. That's exactly what happened in practice during World War II, when the defenses mounted in Leningrad, Moscow, and Stalingrad played a major role in the Allied victory.

But in the current evolution of warfare, cities are no longer defensive anchors against armored thrusts ranging through the countryside. They have become the main targets of offensive action themselves. Just as the huge militaries of the early twentieth century were vulnerable to supply and communications disruption, cities are now so heavily dependent on a constant flow of services from various centralized systems that even the simplest attacks on those systems can cause massive disruption.

Most of the networks that we rely on for city life—communications, electricity, transportation, water—are overused, interdependent, and extremely complex. They developed organically as what scholars in the emerging field of network science call "scale-free networks," which contain large hubs with a plethora of connections to smaller and more isolated local clusters. Such networks are economically efficient and resistant to random failure—but they are also extremely vulnerable to intentional disruptions, as Albert-Laszlo Barabasi shows in his important book *Linked: The New Science of Networks*. In practice, this means that a very small number of attacks on the critical hubs of a scale-free network can collapse the entire network. Such a collapse can occasionally happen by accident, when random failure hits a critical node; think of the huge Northeast blackout of 2003, which caused $6.4 billion in damage.

Further, the networks of our global superinfrastructure are tightly "coupled"—so tightly interconnected, that is, that any change in one has a nearly instantaneous effect on the others. Attacking one network is like knocking over the first domino in a series: it leads to cascades of failure through a variety of connected networks, faster than human managers can respond.

The ongoing attacks on the systems that support Baghdad's 5 million people illustrate the vulnerability of modern networks. Over the last four years, guerrilla assaults on electrical systems have reduced Baghdad's power to an average of four or five hours a day. And the insurgents have been busily finding new ways to cut power: no longer do they make simple attacks on single transmission towers. Instead, they destroy multiple towers in series and remove the copper wire for resale to fund the operation; they ambush repair crews in order to slow repairs radically; they attack the natural gas and water pipelines that feed the power plants. In September 2004, one attack on an oil pipeline that fed a

power plant quickly led to a cascade of power failures that blacked out electricity throughout Iraq.

Lack of adequate power is a major reason why economic recovery has been nearly impossible in Iraq. No wonder that, in account after account, nearly the first criticism that any Iraqi citizen levels against the government is its inability to keep the lights on. Deprived of services, citizens are forced to turn to local groups—many of them at war with the government—for black-market alternatives. This money, in turn, fuels further violence, and the government loses legitimacy.

Insurgents have directed such disruptive attacks against nearly all the services necessary to get a city of 5 million through the day: water pipes, trucking, and distribution lines for gasoline and kerosene. And because of these networks' complexity and interconnectivity, even small attacks, costing in the low thousands of dollars to carry out, can cause tens of millions and occasionally hundreds of millions of dollars in damage.

Iraq is a petri dish for modern conflict, the Spanish Civil War of our times. It's the place where small groups are learning to fight modern militaries and modern societies and win. As a result, we can expect to see systems disruption used again and again in modern conflict—certainly against megacities in the developing world, and even against those in the developed West, as we have already seen in London, Madrid, and Moscow.

Another growing threat to our cities, commonest so far in the developing world, is gangs challenging government for control. For three sultry July days in 2006, a gang called PCC (Primeiro Comando da Capital, "First Command of the Capital") held hostage the 20 million inhabitants of the greater São Paulo area through a campaign of violence. Gang members razed police stations, attacked banks, rioted in prisons, and torched dozens of buses, shutting down a transportation system serving 2.9 million people a day.

The previous May, a similar series of attacks had terrified the city. "The attackers moved on foot, and by car and motorbike," wrote William Langewiesche in *Vanity Fair*. "They were not rioters, revolutionaries, or the graduates of terrorist camps. They were anonymous young men and women, dressed in ordinary clothes, unidentifiable in advance, and indistinguishable afterward. Wielding pistols, automatic rifles, and firebombs, they emerged from within the city, struck fast, and vanished on the spot. Their acts were criminal, but the attackers did not loot, rob, or steal. They burned buses, banks, and public buildings, and went hard after the forces of order—gunning down the police in their neighborhood posts, in their homes, and on the streets."

The violence hasn't been limited to São Paulo. In December 2006, a copycat campaign by an urban gang called the Comando Vermelho ("Red Command") shut down Rio de Janeiro, too. In both cases, the gangs fomenting the violence didn't list demands or send

ultimatums to the government. Rather, they were flexing their muscles, testing their ability to challenge the government monopoly on violence.

Both gangs had steadily accumulated power for a decade, helped in part by globalization, which simplifies making connections to the multitrillion-dollar global black-market economy. With these new connections, the gangs' profit horizon became limitless, fueling rapid expansion. New communications technology, particularly cell phones, played a part, too, making it possible for the gangs to thrive as loose associations, and allowing a geographical and organizational dispersion that rendered them nearly invulnerable to attack. The PCC has been particularly successful, growing from a small prison gang in the mid-nineties to a group that today controls nearly half of São Paulo's slums and its millions of inhabitants. An escalating confrontation between these gangs and the city governments appears inevitable.

The gangs' rapid rise into challengers to urban authorities is something that we will see again elsewhere. This dynamic is already at work in American cities in the rise of MS-13, a rapidly expanding transnational gang with a loose organizational structure, a propensity for violence, and access to millions in illicit gains. It already has an estimated 8,000 to 10,000 members, dispersed over 31 U.S. states and several Latin American countries, and its proliferation continues unabated, despite close attention from law enforcement. Like the PCC, MS-13 or a similar American gang may eventually find that it has sufficient power to hold a city hostage through disruption.

The final threat that small groups pose to cities is weapons of mass destruction. Though most of the worry over WMDs has focused on nuclear weapons, those aren't the real long-term problem. Not only is the vast manufacturing capability of a nation-state required to produce the basic nuclear materials, but those materials are difficult to manipulate, transport, and turn into weapons. Nor is it easy to assemble a nuke from parts bought on the black market; if it were, nation-states like Iran, which have far more resources at their disposal than terrorist groups do, would be doing just that instead of resorting to internal production.

It's also unlikely that a state would give terrorists a nuclear weapon. Sovereignty and national prestige are tightly connected to the production of nukes. Sharing them with terrorists would grant immense power to a group outside the state's control—the equivalent of giving Osama bin Laden the keys to the presidential palace. If that isn't deterrent enough, the likelihood of retaliation is, since states, unlike terrorist groups, have targets that can be destroyed. The result of a nuclear explosion in Moscow or New York would very probably be the annihilation of the country that manufactured the bomb, once its identity was determined—as it surely would be, since no plot of that size can remain secret for long.

Even in the very unlikely case that a nuclear weapon did end up in terrorist hands, it would be a single horrible incident, rather than an ongoing threat. The same is true of dirty bombs, which disperse radioactive material through conventional explosives. No, the real long-term danger from small groups is the use of biotechnology to build weapons of mass destruction. In contrast with nuclear technology, biotech's knowledge and tools are already widely dispersed—and their power is increasing exponentially.

The biotech field is in the middle of a massive improvement in productivity through advances in computing power. In fact, the curves of improvement that we see in biotechnology mirror the rates of improvement in computing dictated by Moore's Law—the observation, borne out by decades of experience, that the ratio of performance to price of computing power doubles every 24 months. This means that incredible power will soon be in the hands of individuals. University of Washington engineer Robert Carlson observes that if current trends in the rate of improvement in DNA sequencing continue, "within a decade a single person at the lab bench could sequence or synthesize all the DNA describing all the people on the planet many times over in an *eight-hour day*." And with ever tinier, cheaper, and more widely available tools, a large and decentralized industrial base that is hiring lab techs at a double-digit growth rate, and the active transfer of knowledge via the Internet (the blueprints of the entire smallpox virus now circulate on the Web), biotech is too widely available for us to contain it.

In less than a decade, then, biotechnology will be ripe for the widespread development of weapons of mass destruction, and it fits the requirements of small-group warfare perfectly. It is small, inexpensive, and easy to manufacture in secret. Also, since dangerous biotechnology is based primarily on the manipulation of information, it will make rapid progress through the same kind of amateur tinkering that currently produces new computer viruses. Terrorists also have a growing advantage in delivering bioweapons. The increasing porousness of national borders, size of global megacities, and volume of air travel all mean that the delivery and percolation of bioweapons will be fast-moving and widespread—potentially on several continents at once.

It is almost certain that we will see repeated, perhaps incessant, attempts to deploy bioweapons with new strains of viruses or bacteria. Picture a Russian biohacker who, a decade from now, designs a new, deadly form of the common flu virus and sells it on the Internet, just as computer viruses and worms get sold today. The terrorist group that buys the design sends it to a recently hired lab tech in Pakistan, who performs the required modifications with widely available tools. The product then ships by mail to London, to the awaiting "suicide vectors"—men who infect themselves and then board airplanes headed to world destinations, infecting passengers on the planes and in crowded terminals. The infection spreads quickly, going global in days—long before anyone detects it.

It's very possible that many cities will fall in the face of such deadly threats. Megacities in the developing world—which often, because of their rapid growth, widespread corruption, and illegitimate governance, aren't able to provide security or basic services for their citizens—are particularly vulnerable. However, cities in the developed world that properly appreciate the threats arrayed against them may devise startlingly innovative solutions.

In almost all cases, cities can defend themselves from their new enemies through effective decentralization. To counter systems disruption, decentralized services—the capability of smaller areas within cities to provide backup services, at least on a temporary basis—could radically diminish the harmful consequences of disconnection from the larger global grid. In New York, this would mean storage or limited production capability of backup electricity, water, and fuel, with easy connections to the delivery grid—at the borough level or even smaller. These backups would then provide a means of restoring central services rapidly after a failure.

Similarly, cities may combat networked gangs by decentralizing their own security. Cities have long maintained centralized police forces, but gangs can often overwhelm them. Many governments are responding with militarized police: China is building a million-man paramilitary force, for example; and even in the United States, the use of SWAT teams has increased from 3,000 deployments a year in the 1980s to 50,000 a year in 2006. But militarized police may too easily become an army of occupation, and, if corrupt, as they are in Brazil, they may become enemies of the state along with the gangs.

A better solution involves local security forces, either locally recruited or bought on the marketplace (such as Blackwater), which can be powerful bulwarks against small-group terrorism. Such forces may become a vital component in our defense against bioterrorism, too, since they can enforce local containment—and since large centralized services, like the ones we have today, might actually accelerate the propagation of bioweapons. Still, if improperly established, local forces can also become rogue criminal entities, like the Autodefensas Unidas de Colombia and the militias in Rio de Janeiro. Governments need to regulate them carefully.

In the future, we probably won't know exactly how we will be attacked until it happens. In highly uncertain situations like this, centralized solutions that emphasize uniform responses will often collapse. Heterogeneous systems, by contrast, are unlikely to fail catastrophically. Moreover, local innovation—supplemented by a marketplace in goods and services that improve security, detection, monitoring, and so on—is likely to develop responses to threats quickly and effectively. Other localities will copy those responses that prove successful.

In June 2007, the FBI and local law enforcement halted a plot to blow up the John F. Kennedy International Airport's fuel tanks and feeder pipelines. This was another great

example of how police forces, if used correctly, can defuse threats before they become a menace [see "On the Front Line in the War on Terrorism"]. However, our current level of safety will not last. The selection of the target demonstrated clearly that future attackers will take advantage of our systems' vulnerability to disruption, which will sharply increase the number of potential targets. It also showed that these threats can emerge spontaneously from small groups unconnected to al-Qaida. More and more attempts will come, with higher and higher rates of success. Our choice is simple: we can rely exclusively on our current security systems to stop the threats—and suffer the consequences when they don't—or we can take measures to mitigate the impact of these threats by exerting local control over essential services.

****

This article was originally published in the Summer Edition of ***City Journal***. http://www.city-journal.org/html/17_3_urban_terrorism.html

John Robb , is a former U.S. counterterrorism operations planner and commander. He now advises corporations on the future of terrorism, infrastructure and markets. He is a graduate of Yale University and the United States Air Force Academy.

His writing can be found at *Global Guerrillas; Networked tribes, infrastructure disruption, and the emerging bazaar of violence. An open notebook on the first epochal war of the 21st Century*. (www.globalguerrillas.typepad.com/).

His recent book is Brave New War.