THE FUTURE OF

NEUTRON CAMERAS VERSUS SMUGGLED NUCLEAR BOMBS.
BIODETECTORS VERSUS BIOENGINEERED SMALLPOX.
IS TECHNOLOGY MAKING US SAFER—OR MORE VULNERABLE?

By the editors of Discover

AT THE END OF A LONG HALLWAY IN A GRAY AND CAVERNOUS BLOCK
at the University of Arizona in Tucson sits a closet-size room secured by complex
access codes and bulletproof-glass windows. The room is chilled to a steady 60
degrees and crammed with rack-mounted monitors, blinking red lights, a squat
supercomputer, and three “spidering machines” that crawl through the Internet,
quietly spooling data from the shadowy digital realm inhabited by terrorists, hack-
ers, and cybercriminals. Welcome to the Dark Web.

These machines store Web data from roughly 1,500 terrorist and extremist orga-
nizations, including 500 groups with roots in the Middle East, explains University
of Arizona computer scientist Hsinchun Chen, who designed this digital sleuthing
tool. Accessible only to those who pass fingerprinting and extensive background
checks, the Dark Web project constitutes the largest collection of online terrorist
data on the planet and may be key to cracking future plots. It is, literally and meta-
phorically, a portal to the underworld.

Tall and affable, Chen is just one among thousands of scientists and government
agents working doggedly to infiltrate terrorist networks around the world and to
disrupt their actions. The expansion of the Web and wireless technology, open-
source coding, and free online storage have been a boon to terrorist organizations.
More than simply a communication tool, the Web serves as a platform for e-jihad:
TERRORISM
SECURING THE SKIES Armed officers patrolling airports have become an unremarkable sight since 9/11. Baggage is scanned, checked, and sealed.
planning, recruitment, fund-raising, training, and indoctrination. The number of jihadist Web sites has grown from a dozen in 1998 to 4,800 today. “They know how to use the Internet in an intelligent way,” says a member of Chen’s team. “They’re hiding in the shadows,” adds Chen.

The Dark Web Project has developed algorithms for assessing the threats associated with various Web sites and forums. One is a mathematical formula that measures the “infectiousness” of ideas on a Web forum. An infectious idea is one that spreads rapidly, like a highly contagious cold. The formula takes into account such parameters as the number of postings, the volume and duration of a conversational thread, and the number of members participating. It then generates a “thread score” that is tracked over time. Some ideas peter out, while others hit a tipping point. The system also uses keyword and textual analysis to quantify and track the level of violence and racial hatred expressed on a Web site or forum—a measure that can be used to determine which groups might be most threatening and to alert investigators to follow up.

Chen’s group has also developed techniques to decipher social interactions among terrorists online. One method, called link analysis, studies the connections between Web sites and online forums to create a two-dimensional map that reveals at a glance the relationships between terrorist clusters. On a monitor, Chen calls one up. It somewhat resembles a map of airport hubs. Small circles represent individuals, some of whom are grouped into rings of teams. Lines radiate from each ring, connecting to other circles with which they are affiliated. A group’s importance can be inferred quickly from the number of lines connected to it. One ring is shaded nearly black with connections. “This was the 9/11 group,” Chen says. “In the middle here, this is Bin Laden.”

Even before the truck bombing of the World Trade Center in 1993, and increasingly since 9/11, public officials and private agents have fretted over the many forms that a terrorist attack might take. As scenarios go, few are as frightening or as plausible as a chemical attack—not a chemical weapon per se but the sabotage of chemical plants found in abundance around most major cities. Such an attack would, like the 9/11 hijackings, take our own technology and turn it into a potent weapon against us.

For a sense of the threat, just drive along the Pulaski Skyway, a heavily traveled stretch of road that leads from New York City through eastern New Jersey. Ironwork trusses rise and fall like primav surges across the Hackensack River, which meanders for miles past warehouses, depots, and storage tanks. Below the elevated roadway stretches a landscape that in 2004 U.S. Attorney Christopher J. Christie called “the most dangerous two miles in America.” This bustling area includes Newark Liberty International Airport, an electrical generating station, oil and gas pipelines, major passenger and freight lines, numerous chemical processing plants, and the ports of Elizabeth and Newark.

Not far off, surrounded by a tall chain-link fence on a dead-end street, stands a chemical plant that processes chlorine gas. According to records at the Environmental Protection Agency, a catastrophic release here could pose a potentially lethal threat to the 12 million people who live within a 14-mile radius. A Discover reporter managed to find the inconspicuous plant, take a few photographs, and spend some moments pondering how fragile the building was and the havoc that could be caused with a single well-aimed truck bomb.

“It’s such a dense population center, and it’s ripe with targets,” says Andrew C. McCarthy, a former supervisor of the U.S. Attorney’s antiterrorism command post in New York City and the federal prosecutor who led the case against Sheik Omar Abdel Rahman.

The risk is mitigated slightly by the fact that experts know about it. But what about what they don’t know—the “unknown unknowns,” as Secretary of Defense Donald Rumsfeld so poetically put it? We think we have a handle on the present state of terrorism, but what about its future? In recent years, counterterrorists have begun making detailed studies of potential new threats and developing an array of advanced technologies to safeguard against them: biosniffers, set up in more than two dozen American cities, that test the air for an indication of dangerous pathogens; neutron and gamma-ray “cameras” that can quickly search shipping containers for smuggled radiological material; and artificial intelligence that sifts heaps of online bank transactions and flags suspicious activity.

Surveillance techniques have also become more powerful, both on the ground and in orbit. (Britain is arguably the leader in conventional camera surveillance, with 500,000 security cameras monitoring public spaces.) According to a Rand Corporation study, law enforcement officials at the 2001 Super Bowl employed a new biometric technology to search for potential terrorists. Surveillance cameras surreptitiously gathered images of faces scanned in the crowd; algorithms then measured various facial features in the images, and the resulting “faceprints” were instantly searched against a computerized database of known suspects and criminals. At the Super Bowl in 2006, agents with the Department of Homeland Security used a newer technology, called LifeVision, which took threedimensional images using binocular surveillance cameras.

Pressed for details on its counterterrorism efforts, the Department of Homeland Security offers a carefully measured statement. “We are harnessing 21st-century technologies in a number of areas...”
TERROR FAMILY TREE Web communications tracked by computer scientists reveal a clear network of relationships among members of terrorist groups (left). Meanwhile, videos of Osama bin Laden (right) appear on the Arabic television station Al Jazeera—a reminder that the terrorists remain one step ahead.

that contribute to the security of the homeland," says Russ Knoke, the agency press secretary. "Improved intelligence gathering and analytical capabilities. We’ve seen tremendous progress in aviation security, in maritime security. But we’re also the first to admit that there is more work to be done."

Many experts note that even the most advanced technologies are useless unless the problem is addressed at its root. "The war on terrorism is really a proxy for saying what is really a war on militant Islam," McCarthy says. "If we’re not willing to take on the ideology and try to develop a reformist, moderate Islam that makes militant Islam a fringe element, we haven’t much hope to stamp it out."

Meanwhile, officials are bracing for a more diverse and technologically savvy enemy than what they have seen before. In its April 2006 report on terrorism, the State Department noted that the leaders of Al Qaeda "are scattered and on the run." Increasingly, the terrorist threat instead comes from "small autonomous cells and individuals" who draw on "advanced technologies and the tools of globalization such as the Internet, satellite communications and international commerce." In the future, McCarthy says, "it will take fewer and fewer people to do more damage."

In popular perception, suicide terrorists are desperate, uneducated naiifs or psychotic dupes. Certainly that applies to some of those who have been caught so far. But the terrorists planning strategies for the future are probably far more astute than those disoriented few. "It’s a Darwinian situation," says Hugh John Williams, a private consultant and a former member of British intelligence. "We catch the less smart ones, and the ones who get away learn from their less fortunate associates."

Psychiatrist Marc Sageman, a former CIA case officer who has worked closely with Afghanistan’s mujahideen, recently completed what is perhaps the only scientific analysis of the social factors that help make a terrorist. Combing court transcripts and other documents, Sageman compiled a database of the motives and backgrounds of 500 jihadists and found that the average terrorist is middle-class, sane, well-informed, and educated. The typical occupation: engineer. Jim Crupi, a military consultant, likens tomorrow’s terrorist group to a Silicon Valley start-up: "value driven, networked, global in scope, and targeted to a niche."

The difference, he adds, is that terrorists don’t have to develop their own technology. "They have a worldwide communications system called the Internet that they did not have to pay for. They can buy computers very cheaply and analyze data, determine targets, coordinate with one another, and pass stuff encrypted in little dots on photographs that they can send with very cheap software. We created their weapons—the computer, the Internet, the files that can carry coded messages."

A nuclear attack is by far the most challenging technological feat for terrorists. Yet Graham Allison, assistant secretary of defense in the first Clinton administration and now director of the Belfer Center for Science and International Affairs at Harvard University, places the odds of a nuclear strike within the next decade at 51–49—slightly worse than the odds of a coin. "A nuclear terrorism attack is inevitable if we continue on the autopilot path we’re on," he says.

And what would such an attack do? Allison has posted the grim answer on his Web site (www.nuclearterror.org), which shows a three-color "blast map" depicting the effects of a 10-kiloton bomb, comparable to the one dropped on Nagasaki and about the smallest a workable nuclear device could be. In the red zone, within one-third of a mile of ground zero, the bomb would destroy buildings, people, and just about anything else; in the green zone, within three-fourths of a mile, people would either die immediately or be seriously injured.
by fire and radiation. For a plausible target like Lower Manhattan, that could easily translate to more than 100,000 fatalities.

There is little question that Al Qaeda is interested in going nuclear. Former CIA analyst Michael Scheuer reports that in 1996 the "CIA's Bin Laden unit acquired detailed information about the careful, professional manner in which al-Qaeda was seeking to acquire nuclear weapons." In 2003 Bin Laden made the dramatic gesture of requesting a fatwa from a radical Saudi cleric authorizing the use of a nuclear bomb against American civilians (not surprisingly, his request was granted).

Allison has some good news as well. The image of a clandestine terror group buying an old Soviet nuke on the black market is almost certainly a Hollywood fantasy. Despite the chaos following the breakup of the Soviet Union—which left 18,000 nuclear warheads in the hands of a group of new nations—there is no evidence that any of our old adversary's tactical or strategic nuclear weapons ever left government control. Allison credits the furious work by the American and former Soviet governments, accomplished partly under his watch: "Had nothing been done, there would already have been a nuclear attack."

It is now highly unlikely that any rogue organization could get its hands on an existing nuclear weapon, because the devices are well-guarded and have fail-safe protective mechanisms that no amateur is likely to crack. Russian officials admit that terrorist teams managed to carry out reconnaissance on two nuclear warhead storage facilities and two nuclear-weapon transport trains in 2001 and 2002, but the teams apparently never came close to being able to steal them.

Building a nuclear bomb from scratch would be a huge undertaking for any terrorist cell, which is why some other security analysts see less nightmarish odds than Allison does. A group of international security experts polled by Senator Richard Lugar puts the average probability of a nuclear attack on U.S. soil within a decade at around 29 percent, still pretty terrifying. Mathew Bunn, one of Allison's colleagues at Belfer, places the risk at more like 5 to 10 percent—high enough to make it the top national-security concern.

The problem is that the nuclear cat is out of the bag. These days, finding bomb-building instructions is comically easy. Two declassified U.S. government publications, based on the work of Manhattan Project scientists, offer detailed guidance. Both are available on Amazon.com for a total of $40.76, plus shipping.

Transforming those plans into reality would require a minimum of 50 pounds of highly enriched uranium, about 1,500 carefully machined parts, a nuclear design engineer, and more than a dozen craftsmen able and willing to put the device together. A. Q. Kahn—the so-called father of the Pakistani atomic bomb program—may have sold portions of that nation's nuclear technology to Libya and perhaps to terror groups as well, according to an Institute for Science and International Security report. As for fissile material, Russia is deemed a major nuclear-supply risk because it has large amounts of enriched uranium stashed away. Security of nuclear materials worldwide "ranges from 'better than probably necessary' to 'absolutely appalling bad,'" Bunn says.

The situation in Russia is improving, in part because of the Nunn-Lugar Cooperative Threat Reduction Program, which secures and stores fissile materials in the former Soviet Union or defuses them. The Megatons to Megawatts program has secured 269 metric tons of highly enriched uranium and turned it into reactor fuel. On the other hand, the stuff keeps turning up in unexpected places, such as Uzbekistan, where the International Atomic Energy Agency recently recovered three bombs' worth of highly enriched uranium. "What the heck are three bombs' worth doing in Uzbekistan?" asks Allison. Recent reports mention other countries—including Ghana, Belarus, and South Africa—that have nuclear material they shouldn't.
Former prosecutor Andrew McCarthy thinks Allison may be focusing on the wrong nuclear fear. Triggering nationwide panic wouldn’t require a nuclear explosion. A dirty bomb—radioactive material scattered by a conventional explosive—“is much less of a problem to detonate and if successful would render a large swath of a big city uninhabitable for years,” he says. Raw materials are far easier to obtain. Dirty bombs don’t need exotic enriched uranium; any highly radioactive material will suffice. Millions of such sources are scattered around the world, including in hospitals that use radioactive isotopes for the treatment of cancer and in radioisotope thermolectric generators, or RTGs, that power remote Soviet installations with the heat produced by nuclear decay.

The impact of a dirty bomb would be far less than that of a true nuclear device. “It is likely that very few Americans will be killed directly, suffer radiation sickness, or even have a measurably increased risk for cancer from an attack,” Peter D. Zimmerman and Cheryl Loeb write in “Dirty Bombs: The Threat Revisited,” a report published by the Center for Technology and National Security Policy at the National Defense University. The primary threat of a dirty bomb would be the economic fallout. Cleaning up the radiation would entail ripping down all contaminated structures and sending them to a special dump. A dirty-bomb attack on a major American city could easily cost more than the $30 billion of the 9/11 attacks, Zimmerman and Loeb conclude.

One solution is to develop better tools for cleaning up a deliberate radiation release. Researchers at Los Alamos National Laboratory are working on a sprayable foam that would bind to radium, cesium, and strontium, likely components of a dirty bomb. When peeled off buildings, the foam would take most of the radiation with it.

A much better way to confront a nuclear or dirty-bomb terrorist attack is to keep radioactive ingredients from getting inside the nation’s borders in the first place, and here physics is on our side. Radioactive materials, by their very nature, emit gamma rays or other distinctive radiation signatures.

After 9/11, U.S. Customs and Border Protection launched what it calls the Container Security Initiative to search for nuclear materials and other terrorist threats before they enter the United States. The program scans for gamma rays and neutrons and performs X-rays of the contents of high-risk cargo in 44 foreign ports, which collectively handle 77 percent of the containers entering the United States. Because of the limited capacity of current scanners, however, only 17.5 percent of that high-risk cargo actually got scrutinized. In April 2005, the Department of Homeland Security founded the Domestic Nuclear Detection Office to add a second layer of security, this time on American soil. That new office recently deployed 214 radiation monitors that scan for gamma rays and neutrons at the “choke point,” where the containers are unloaded. More than 600 such scanners are scheduled for deployment by late 2007.

Current scanning systems generate a lot of false alarms that require investigation, drastically slowing the screening process. They can also be fooled by radiation-absorbent shielding, like lead, that soak up low-energy gamma rays. Dennis Slaughter, a nuclear physicist at Lawrence Livermore National Laboratory in Livermore, California, is therefore developing a smarter scanner that seeks radioactive material actively, not passively. His device—which his team calls a nuclear car wash—fires a beam of neutrons into the item to be examined. If the neutrons hit uranium or any other fissile material, they will release gamma rays energetic enough to pass through most types of shielding. These high-energy rays are also easily distinguished from normal background radiation, cutting down on false positives. Livermore is partnering with General Electric to build a production version.

At Brookhaven National Laboratory on Long Island, nuclear physicist Peter Vanier and his colleagues have created a complementary device tuned to pick out smuggled plutonium, a likely component of a nuclear bomb. Not only can it find hidden nuclear material, Vanier’s detector can also take a rough image of it. The Brookhaven scanner functions much like a pinhole camera for nuclear snapshots and looks like one, too—little more than a decorated box. Its “lens” is a series of square holes that project incoming neutrons onto two gold-plated tungsten wires, each just 12 microns (0.000 inch) thick, in the back of the camera. The scanner also incorporates a circuit board lined with copper strips and enclosed in a chamber pressurized with
helium-3, a rare isotope that reacts strongly with neutrons. Plutonium emits a steady stream of neutrons that, unlike most gamma rays, can penetrate several inches of lead shielding. Some of those escaping neutrons will then smash into other atoms, shaking them and setting loose an electric charge. The metal sheets in Vanier's camera act as electrodes to multiply and detect those neutron-triggered charges. "If you suddenly see neutrons coming over the bridge," Vanier says with the careful understatement of a federal scientist, "you'd be concerned." His plutonium detector is still in the experimental stage, however, and is probably years away from practical use.

If American security forces intercept nuclear material being smuggled into the country, another technology will come into play: nuclear forensics. Every nuclear sample has a host of distinctive attributes, including the exact mix of impurities, the ratio of different radioactive isotopes, even embedded carbon compounds that indicate the sample's age. Using such clues, German police in 1996 traced a cache of mysterious nuclear pellets to one of just two nuclear manufacturing plants, one in Russia and the other in Kazakhstan. Russian officials now keep a database of forensic characteristics of all major nuclear stockpiles in the country to better track down any material if it is ever stolen.

Allison summarizes the problem as "follow the golf clubs or follow the drugs." An American who buys golf clubs abroad and doesn't want to declare them can send them via a company that packs them in a shipping container, which then slips them into port without ever being seen by customs agents; the ability of drug dealers to bypass even the most elaborate border controls is a well-known problem. We are engaged in a high-stakes game of hide-and-seek, Allison says, "and it is inherently easier for hiders than seekers."

In a May 2 speech Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, emphasized that "we cannot become complacent" about microbial threats. A recent article in IJS: A Journal of Law and Policy for the Information Society notes that the "financial, intellectual, and material barriers to bioterrorism are falling at a faster rate than other WMD threats. It is already estimated that the cost of killing one person with a biological weapon is $1... The lethality of infectious diseases provides a uniquely tempting and accessible force of destruction for terrorists."

The revolution in molecular biology has brought it with an array of tools for tinkering with infectious pathogens. Not only can molecular biologists swap genes in and out of organisms to increase their virulence or resistance to antibiotics, they can now assemble entire pathogens from scratch. In 2002 scientists at the State University of New York at Stony Brook unveiled a poliovirus synthesized over a three-year period using nothing but chemicals purchased on the open market. A year later, a team at the J. Craig Venter Institute assembled a virus of similar complexity in just three weeks.

Concern over this technology's potential misuse has prompted Harvard University geneticist George Church to suggest that instruments used to string together DNA sequences should be registered and regulated; Interpol heartily seconded the idea. Although bioengineering probably lies well beyond the capabilities of a typical terrorist, one rogue biologist could wreak devastation. "I'm less worried about terrorists becoming biologists than biologists becoming terrorists," says Gerald Epstein, senior fellow at the Homeland Security Program at the Center for Strategic and International Studies in Washington, D.C.

Scientific literature is thick with examples of well-intended experiments gone awry that yielded results only a terrorist could love. While trying to come up with a contagious method of birth control among rodent pests, an Australian lab in 2001 modified a mousepox virus, which unexpectedly caused the rodents' immune system to fail completely—even in animals previously vaccinated against mousepox. Because the results hinted that human viruses might be similarly manipulated, a debate broke out over whether publishing such results would aid terrorists. A more recent incident—the 2005 publication in the journal Science of the sequence of the 1918 flu virus, which killed more than 20 million people—prompted computer pioneers Ray Kurzweil and Bill Joy, in a New York Times op-ed article, to rail against too much scientific openness.

Some of the most alarming experiments demonstrate that genetically engineered biological agents can provoke irreversible changes in the nervous system and the brain. During the 1980s a Soviet bioweapons lab altered a pneumonia-causing bacterium so that in addition to causing respiratory illness, it could also prompt an immune response to myelin, the sheathing on the nerves. Over time, the pneumonia would pass, but the impact on the nervous system would resemble multiple sclerosis—for which there is no cure. Other potential nightmares involve biologists creating customized viruses that can target critical cognitive circuitry, selectively inducing paranoia, engendering calm, or obliterating memory.

And then there are microorganisms that could do devastating damage outside the human body. In one of the most disturbing scenarios, metal-eating microbes could be exploited to infest and destroy computers.

"The ultimate computer virus would be one that did not just eat code but the components of machines," says Eileen Choffnes, study director for the National Research Council and the Institute of Medicine's recent report, "Globalization, Biosecurity, and the Future of the Life Sciences." Strains of bacteria like Shewanella oneidensis have been developed with funding from the Department of Energy to clean up contaminated weapons facilities. The organisms thrive
in toxic environments and metabolize metal. They could easily consume the exposed leads on a computer. Superbugs of the future might also be able to degrade the plastic that encases chips.

Fortunately, imagining custom-engineered microbes is far easier than actually producing, handling, and dispersing them. Craig Venter scoffs at the idea that terrorists would go to the trouble of devising a synthetic bacterium or virus. “Instruments like the DNA synthesizer have been available for 50 years. It’s not a new technology. If somebody wanted to do harm to the population or the planet, they would make antibiotic-resistant infectious agents. That’s something any high school biology class can do.”

David Franz, director of the National Agricultural Biosecurity Center at Kansas State University and a former specialist on biological weapons for the U.S. Army Medical Research Institute of Infectious Diseases, worries that smallpox, although extinct in the wild, could reemerge if theft occurred in the two facilities that still keep samples. And foot-and-mouth disease, although it does not infect people, could devastate the economy if set loose among livestock. Countermeasures against these threats already exist. “We now have enough vaccine for smallpox to immunize the population,” Franz says, “and that happens to be a vaccine that you can give after the fact, for three or four days. We have vaccines now for anthrax and antibiotics for anthrax, and we have some stockpiles and a lot of other preparations for foot-and-mouth disease.”

Since the 9/11 attacks, funding for biodefense research and public-health preparedness has soared from $418 million in 2001 to more than $5 billion in 2006. Before the funding, some local health departments did not even have computers. To scout for potential attacks and disease outbreaks, the Department of Health and Human Services now monitors patterns of emergency room visits, sales of over-the-counter drugs, and school absenteeism. In the Department of Homeland Security’s BioWatch program, mailbox-size machines gather air in major urban areas to be tested for the DNA of smallpox, anthrax, plague-causing _Yersinia pestis_, and other pathogens on a federal list. The BioShield program, funded with $5 billion over 10 years, will purchase new vaccines, antiviral agents, and antibiotics.

“...If we have these tools,” Venter says, “then bioterrorism goes away as a threat.” Marc Wolfson, public affairs specialist on emergency preparedness for the Department of Health and Human Services, is not quite so confident. “We can develop the best countermeasures in the world, but if they’re not there in time to help treat the patient, then they’re not effective,” he says.

The best countermeasures to bioterrorism, according to Franz, are the same ones already being used to combat ordinary infectious disease: “Supporting the public-health system is crucial because it would be very hard to tell emerging disease from bioterrorism.” Upgrades also would be valuable in protecting public health, regardless of whether any malicious biological agent is released.

“Natural infectious disease is a far greater threat than bioterror,” says Steven Block, a physicist and biologist at Stanford University and a member of the National Research Council’s committee on biowarfare. “We have more people dying of the flu in a hospital in any major city on the weekend than died of anthrax during the entirety of the 20th century. The death toll due to flu is unacceptable. If the government is willing to spend billions on terror, we need to make sure that that money is well spent on the eradication of infectious disease in general.”

Manipulating natural diseases is difficult, but technological infection is a threat the general public is all too familiar with. Some security experts worry that the Internet itself could collapse under terrorist attack. In 1999 the Defense Advanced Research Projects Agency (DARPA), creator of the original Internet, investigated the risk of the network being taken over by a virus or worm. The result of their study was a paper predicting that worms could bring down the Internet in minutes. The study was prescient, but apparently unproductive—a few years later, the notorious “I Love You” virus and several other worms clogged the Web, disrupted ATM services, and infected a nuclear power-plant control system.

A long-term implosion of the Internet is unlikely, says David Kotz, a computer scientist and director of the Institute for Security Technology Studies at Dartmouth College. With its redundancies and distributed architecture—exactly the qualities that make it useful—the Internet is so resilient that it would most likely work well even a few days after a grand attack. But the nightmare scenarios are there all the same. Perhaps one of the oddest springs from a translation of “Chinese Views of Future Warfare,” a collection of reports by Chinese military scholars. It describes “ant robots,” microscopic electromechanical systems that could theoretically creep into electronic equipment, such as key Internet routers, and lurk there for years until they are remotely activated to destroy the circuitry.

Less far-fetched schemes target national security networks with conventional jamming, spamming, or silent spying. In March 1998 the Department of Defense uncovered Moonlight Maze, a cyberespionage campaign that penetrated computer systems at the
ONE NUCLEAR EXPERT PUTS THE ODDS OF A NUCLEAR ATTACK IN THE NEXT DECADE AT 51–49, SLIGHTLY WORSE THAN A COIN TOSS

PREPARING FOR THE WORST
Municipal employees take a decontamination shower during an anthrax training exercise in Antibes, France.

DETECTING DANGER
Neutron detectors (above) being designed at Brookhaven National Laboratory can image radioactive materials found in cargo containers (left) from hundreds of feet away.
Pentagon, the Department of Energy, NASA, and various private universities and research labs. The perpetrators, who were never caught, are thought to have used a mainframe computer in Moscow. For more than two years, they secretly accessed thousands of files, including military intelligence, hardware designs, and troop locations. More recently, there have been reports of ongoing cyber-intrusions on U.S. infrastructure and security networks. These attacks, code-named Titan Rain and apparently originating in China, are being investigated by the FBI.

The fragility of our digital infrastructure—and the ease with which it could be shattered—was highlighted in August 2003, when a power grid overload near Buffalo, New York, blacked out much of the Northeast. “A lot of the power grid is automated by computers, and I’ve heard that in some cases they are connected to the Internet by mistake,” says David Kotz. Another fear is that terrorists might strike at the energy industry’s computerized systems for controlling the flow of oil or natural gas through pipelines. “I’d be surprised if terrorist groups are not thinking about this,” Kotz says.

Despite these fears, a significant terrorist assault on an American computer system has never occurred, and no one has ever died from a computer virus. Terror groups generally lack the means and resources to mount anything but relatively harmless cyberattacks, according to a 1999 study by the Center on Terrorism and Irregular Warfare at the Naval Postgraduate School. Nevertheless, the risk may be growing.

As Generation Y upstarts rise in the ranks, terrorists will most likely become more Cybersavvy in the future, according to Mike Skroch, who runs a team that simulates digital security break-ins at Sandia National Laboratories in Albuquerque, New Mexico. “The current leadership of the terrorist organizations are of a generation that doesn’t trust cyber means of attack,” he says. “Once we see a new generation of leadership that is more comfortable with technology, we’re going to see more of this.” Already e-jihad Web sites exist that teach viewers how to make a virus or hack into a site. And Salafi jihadists recently developed a stand-alone Web browser that searches a self-contained database of 3,000 militant Islamic texts. It’s the jihadist equivalent of a V-chip; it shields readers from the full brunt of the Internet and from any ideas that might challenge the militant ideology.

Among its many technological tricks, the Dark Web project is still a research effort. Its content is not accessible online, although Chen has begun to make the portal available to the FBI and to domestic counterterrorist agencies, and he is working on proposals with other groups. He’s also clearly not the only one monitoring traffic in cyberspace. In May news broke that the National Security Agency has been secretly collecting phone records of tens of millions of Americans in order to detect patterns of terrorist activity, just the latest in a series of revelations of the agency’s expanding telephone and Internet surveillance efforts.

It remains to be seen whether the highly contentious NSA program has actually contributed anything to the tracking and capture of terrorist operatives. Elsewhere, the push is on to apply neural networks and data-mining techniques to better monitor online banking.

“There are many people who think that terrorists might be financing some of their operations through organized crime and identity theft,” David Kotz says.

“It takes a lot of money to keep an ideology alive,” adds Graham Dillon, who heads the financial-crime advisory service at the London branch of the accounting firm KPMG. Dillon, a dapper 33-year-old with a Ph.D. in nuclear physics, claims that one of the best ways to hit terrorists is to aim for the wallet. “The key is to shut down funding,” he says. In the future, such efforts will center on technological advances in artificial intelligence. The only way to monitor the hundreds of millions of transactions that flow through banks every day, he says, “is to give a machine human-type cognition through neural networks, so that it’s trained in past behavior.” Such data mining reportedly helped track down an Islamic terrorist cell two years ago, although Dillon declines to provide specifics. “I can’t tell you because the terrorists will read it and see how we got them. We can’t let them know.”

If terrorism experts agree on anything, it’s that the future of terror will be an extended one. “Do I think we’ll ever stop it?” asks Howard Safir, former New York City police commissioner and now chairman and CEO of the private security firm SafirRosetti. “No. Could we get it to a manageable level? I think we can do that.” By way of reassurance, he adds, “You have as much chance of being a victim of a terrorist attack as of being hit by lightning—probably less of a chance.”

Inside the Pentagon, the fight against terrorism is referred to as “the long war.” Yet long needn’t mean perpetual. “We know from the basis of past periods of terrorism that they don’t last forever,” says Michael Barkun, a political scientist at the Maxwell School in Syracuse, New York. “This is a phenomenon, as troubling as it is, that will turn out to have a beginning, middle, and end.”

Scott Atran, an anthropologist at the University of Michigan and at the National Center for Scientific Research in Paris who has extensively studied suicide terrorism, invokes the ghost of 19th-century anarchism. Beginning in the 1880s, a loose, worldwide movement

continued on page 76
arose, dedicated to the elimination of the power of the state and international capital. Anarchist assassins killed the president of France, the empress of Austria, the king of Italy, various Russian officials, and—almost exactly 100 years before 9/11—U.S. president William McKinley. The new president, Theodore Roosevelt, declared anarchism to be the incarnation of "evil" and a "foe of liberty." He made the defeat of anarchism an overriding mission. The anarchists have since disappeared as a threat—although a straggling band of them was spotted recently marching down Fifth Avenue past the Discover offices, waving red flags and chanting, "We're not Americans, we're Proletarians!"

Americans have grown accustomed to the idea that military success follows from technological superiority. The Second World War ended with our development and use of the atomic bomb. The cold war broke in our favor, after our relentless accumulation of nuclear gadgetry became too expensive for the Soviet economy to match. But terrorism will not be easily overwhelmed by technology. Amid all the concerns about stealth nuclear attacks, it's easy to forget that terrorism is largely a low-budget, low-tech affair. "Terrorists will pick the low-hanging fruit, the easiest thing that's consistent with their aim," says Steven Block of Stanford. The most spectacular act of terrorism to date was pulled off with box cutters.

Countering terrorism requires more than technological intelligence. What's needed is human intelligence—a better understanding of what terrorists have in mind and why. "The best source of intelligence is somebody who can give you information about something that's going to happen," says Mark Leap, deputy chief of the Los Angeles Police Department and head of its counterterrorism and criminal intelligence bureau. "People who are planning terrorist acts are going to be disrupted using the same tools we use to catch burglars, robbers, and car thieves: information from the public, detection of low-level criminal activity, a smart beat cop who notices something out of place and conducts an investigation. Timothy McVeigh was caught because he didn't have a front license plate on his car."

Last year, Los Angeles law enforcement authorities arrested four members of a militant Islamic group who were plotting shooting sprees, one timed for the anniversary of 9/11 and another for a Jewish High Holiday. Agents were clued in to them after a series of convenience-store robberies; a warrant turned up fundamentalist writings and a list of targets, including military recruitment offices, synagogues, and the Israeli consulate. The suspects had ordered an assault rifle; they were arrested during California's mandatory 10-day waiting period for guns.

Understanding how terrorist groups form is another important way of subverting their aims, says psychiatrist Marc Sageman. By and large, the terrorists Sageman studied were young men who were egged on in their fanaticism not by some distant, multi-tentacled organization but by members of their own tight-knit cells. Typically marginalized by society, often underemployed, they sought a cause that would give them "social community and a reason for self-sacrifice." Some fell in with the cause at extremist mosques and then became further radicalized in groups of friends or relatives.

"The young, idealistic people are trying to build a better world—this is for justice and fairness," Sageman says. "And their belief is that the world has only been just at the time of the Prophet and his companions. That's what they're trying to build. There are many ways to do that—there are some peaceful ways. But young people are often in a hurry, and that's where violence comes in." Sageman and Scott Atran contend that with tactful intervention destructive energy might be diverted toward more positive goals. Atran proposes infiltrating chat rooms on jihadist Web sites and advancing causes that "play to jihadist sentiments but are not destructive, such as providing faith-based social services."

Perhaps more than any war the United States has ever fought, the fight against terrorism is a war of ideas. To that end, the most advanced technologies that terrorists have at their disposal are ones that Americans know well: television and online media. "Essentially, it's an image war," says Graham Dillon of KPMG. "PR is everything in terrorism. Why? Look at what the terrorists are trying to achieve: political or ideological change. And if people don't buy into a doctrine, the terrorists can't succeed."

In the view of some experts, terrorism brings with it another worry—the threat of overreacting to it. Atran fears that a nuclear attack on the United States could prompt a geopolitical chain reaction. "There would be enormous pressure for an immediate and devastating political response. Three Algerians from Paris blow up a bomb in Washington; we vaporize Tehran and get rid of everybody we don't like: anyone who's strategically culpable, whom we believe supports terrorism or sponsors it. If that happens, the world would be as different a place as after World War II."

Even in less extreme scenarios, the fight against terrorism has the potential to undermine the principles that the fight claims to uphold. Impressive as the government's new surveillance techniques are, they are sometimes matched by a disconcerting arrogance in using them. The new emphasis on security places potentially self-defeating limits on scientific openness. What unnerves him, Craig Venter says, "are people in op-eds who scream foul about work on the 1918 flu virus being published in the literature, saying we should usher in a new era of secrecy and clamp down on science. We went through this with the government when I was at NIH and we were working on the smallpox sequence." Venter notes that the first agency to benefit from the smallpox-genome data was the CIA, which used it to develop rapid-detection kits.

It may well be impossible to uproot terrorism or to fully insulate ourselves against it. "You can do preventative things," Howard Safir says. "And you can make people safer. You can't make people safe. You are never safe, because in an open and free society you're always vulnerable to people who are extreme."

Reported by Josie Glausiusz, Amos Kenigsberg, Susan Kruglinski, Yasmine Mohseni, Sarah Richardson, Jessica Ruinsky, Jason Stahl, Alex Stone, and Kathy A. Svitil

For expanded interviews and additional material, visit the Discover Web site: www.discover.com.