AL QAEDA AND YOUR WATER

Steven J. Duranceau, PhD, PE
C. David Plavcan, PE
Boyle Engineering Corporation
320 East South Street
Orlando, Florida 32801

Rick Hahn, FBI Retired
R. Hahn & Company, Inc.
Los Angeles, California

William J. Ackerman, Secret Service Retired
Strategic Options
Fort Lauderdale, Florida

A. AL QAEDA, THE TERRORIST INFRASTRUCTURE

Who is al Qaeda? We all know who Osama bin Laden is. The son of a wealthy Saudi construction magnate who's company performed restoration and improvements to the Muslim mosques at Medina and Mecca in the 1970s. Through the process of restoring the mosques, both Osama and his father became very devout Muslims.

When Russia invaded Afghanistan in 1979, Osama, a young devout believer in fundamentalist Islamic philosophy, was anxious to join the fray to drive the "infidels" out of a neighboring Muslim state. The U.S., Britain, and other western powers were only too happy to help, which they did by using Pakistan as a surrogate for support. Hence was born the mujahideen of Afghanistan. After 10 years of war, Russia pulled out. By that time bin Laden had not only distinguished himself as a fearless battlefield commander, he had spent much of his own fortune organizing recruitment and training for the "Arab Afghans", volunteers to fight in Afghanistan.

Bin Laden returned to Saudi Arabia, where he became a popular orator at mosques, preaching the evils of the infidels, particularly the west, and the power of Allah. He, like most fundamentalists, was distressed when the Saudi government allowed U. S. Troops onto the soil of Saudi Arabia, the holiest ground of Islam. The Saudi Royal family did their best to assure the citizenry that the situation was only temporary, designed to address Iraq's invasion of Kuwait. But bin Laden continued to speak out against the House of Saud. He became more and more vociferous as the "Desert Shield" operation unfolded into "Desert Storm." The concept that Arab states would break ranks among themselves, and some join forces with the hated west to oppose another Arab state, was a shocking calamity. The time of the Gulf War, as it is known in the west, is referred to as al-Azma, "the Crisis" in the Muslim world.

When the war ended, Saudi Arabia decided to allow U. S. forces to remain in the country. The decision, they knew, would alienate the fundamentalists in the populace, but they too feared Iraq. Bin Laden became more vitriolic toward his own government. Consequently the government increased pressure on bin Laden to be silent. The result was that bin Laden went into exile in Sudan in 1991. Working with Sudan's spiritual leader, Hassan Abdallah al-Turabi, bin Laden and others set about utilizing the network of trained "Afghan Arabs" they had at their disposal to oppose western presence in the Muslim world.

In the years between 1991 and 2001, bin Laden aligned with a number of other leaders of various organizations that had terrorist cells to engaged in efforts to attack and impact the U. S. Among those

who joined with him in these efforts was Ayman, Zawahiri, an Egyptian doctor-turned-terrorist, who was a leader in the Egyptian Jihad, the group believed responsible for the 1981 assassination of Egyptian President Anwar Sadat. Another was Ahmed Taha Musa-a – leader of Al Gama'a al Islamiyya – also and Egyptian group. Al Gama'a al Islamiyya is the group that Sheik Rahman, formerly the leader of a mosque in New Jersey, is spiritual leader of. Still another of bin Laden's new found allies was Maulana Rehman Kalil – Leader of Harkat Mujahideen of Pakistan, a group that had been involved in terrorism on the Pakistan – India border for years.

Together, these groups started an organized campaign to drive westerners, particularly the military forces, from the Arabian Peninsula. The acts attributed to them collectively over the next ten years include the driving of U. S. forces from Somalia, as depicted in the movie "Blackhawk Down"(1993); the 1993 bombing of the World Trade Center, the bombing of the Military Cooperation Program Building in Rhyadh, Saudi Arabia (1995); the slaughter of 67 western tourists at an archeological site in Luxor, Egypt (1997), the bombing of U. S. Embassies in Tanzania and Kenya (1998), and the bombing of the USS Cole (2000).

Clearly, bin Laden and the fundamentalists aligned with him mean great harm to the western powers, and the U. S. in particular. What was once the "Arab Afghans" or mujahideen that the west supported, have evolved into a tool of terror known as al Qaeda. Perhaps the best statement of their intent is crystallized in the religious edict issued by bin Laden in February, 1998. Referred to as a "fatwa", it states in part:

"To kill Americans and their allies – civilian and military – is an individual duty for every Muslim who can do it in any country in which it is possible to do it."

The four signers to this "fatwa" are Zawahiri, Taha Musa-a, Kalil and Mir Hamza, - a Pakistani religious leader and supporter of the Taliban who endorses attacking the U. S.

Since September 11th, we, the citizenry of the U. S., live in a changed world. The tragic events of September 11th, 2001, were applauded by Islamic fundamentalists, as it brought the war to America's shores in a dramatic, spectacular way. With our increased presence in the Arab world, and the prospect of war with Iraq looming, it is predictable that the terrorists will continue to attack us, both abroad and at home. Unfortunately, the more dramatic, spectacular, and costly to us a terrorist event could be, the more appealing it will be to them. We are, indeed, at war, and as in any conflict, the possibility of disrupting the enemy by "poisoning the well" may be a tactic al Qaeda entertains.

B. TERRORIST INCIDENTS AND INTELLIGENCE

In answering the question of how real the threat to our water supplies is from al Qaeda, we need to examine two things; first, whether or not there is evidence to indicate that the poisoning of water, or other attacks on water systems, is a tactic al Qaeda has examined; and second whether there is evidence to indicate that al Qaeda, or any related group has attempted such an attack.

Although there have been no reports of successful contamination of water, there have been a number of plots, both inside and outside the U.S. reported wherein Muslim extremists reportedly planned to contaminate the water. Some of these incidents include:

On February 20th, 2002, four Moroccans in possession of 4 kg of potassium ferrocyanide (PF) were arrested in Rome. The report, cited here, states "The significance of this arrest was underscored by the fact that the terrorists were also in possession of detailed maps of the US embassy, the Rome water supply network and reports that 100 false residence permits were also found."[1] By the following Sunday,

February 24th, the number of persons in custody climbed to nine. CNN reported that the raid at the Rome apartment turned up a map of the city's underground waterworks, with the location of the U.S. Embassy circled. It also reported "Authorities launched a search of the utility tunnels depicted on the map. On Sunday, the U.S. State Department said it had discovered at least one hole carved into a tunnel near the U.S. Embassy in Rome." and "Sources familiar with the investigation said the hole was large enough for a very small person to squeeze through." The article ends noting "no link so far has been established between the hole found near the embassy and the arrests of the nine being questioned." [2]

This incident occurred just a few weeks after the arrest of a Milan, Italy based terrorist cell, which is believed to be linked to al Qaeda. One of the men arrested in Rome was reported as related to the Milan cell. A conversation of a member of the Milan cell reportedly was electronically intercepted in which he is speaking to a Libyan, Ben Hani Lased, known as "the chemist", about use of chemical substances in terrorist attacks. Reports indicated that the Milan cell "used the phrase 'tomato cans' which intelligence sources claim was a code word for cyanide." [3] According to a report by Radio Netherlands, "In one conversation, he told a Libyan associate that there was a plan to 'try out' a drum of a 'liquid' in France. 'This liquid is more efficient because as soon as it opens, people are suffocated,' he was quoted as saying." [4]

In addition to the Rome and Milan incidents, there have been two reported incidents of foreign, or foreign influenced entities within the United States that demonstrated interest in water contamination. One was reported simultaneous interest on the part of a middle-eastern man in the water system and diseases transmutable from animals to humans, in Canton, Ohio. This was reported in October, 2001 in a local Canton newspaper. The story states "An associate of two men indicted in Detroit in the terrorist investigation did library research on a water system and animal-born diseases, the Akron Beacon Journal reported.

The newspaper said in its Friday editions that the man, who had identified himself at the Stark County District Library last summer as an Egyptian, asked for detailed maps of Canton's city water system and books on parasites and diseases that can be passed from animals to people." The local librarian reported the incident and identified the event as occurring during the summer of 2001. The report further identifies the "Egyptian" as living and working in the Canton area with two individuals who subsequently moved to Detroit, and were arrested for "fraud and misuse of visas, permits and other documents." The article identifies the Detroit associates as Karim Koubriti, and Ahmed Hannan. [5]

Nearly a year later, on August 28, 2002, the U. S. Justice Department announced indictment of Koubriti, Hannan and three others on "charges of conspiracy to provide material support or resources to a terrorist organization linked to al Qaeda." and "The men, whom authorities say have lived in the United States since at least 2000, were charged with operating a "sleeper" cell that operated as 'a covert underground support unit for terrorist attacks within and outside the United States'." The article reports they are also "accused of trying to 'directly access airlines' by finding security breaches at Detroit Metropolitan Airport. Some worked in the kitchen of an airline catering firm, while others were experts in the use of fake IDs and calling cards. At least one received funds and consulted with a network of other "brothers" in Europe linked to a fundamentalist Islamic religious movement called Salafiyya, the indictment said." [6]

Although this report makes no more reference to the individual who made the curious inquiry in Canton, Ohio a year before, this report does state that "Four of the men were held soon after Sept. 11, while the man identified as Abdella remains a fugitive." It also states "The indictment did not spell out any specific charges against Hmimssa because he is cooperating in the investigation, a federal law enforcement official said."[6] Consequently, we are left to speculate as to whether the fugitive Abdella, or the cooperating subject, Hmimssa, may have been the mysterious visitor to the Ohio library. Nonetheless, clearly the incident has been linked by the FBI to suspected al Qaeda supporters.

Yet another reported water related threat posed by terrorists inside the U. S., involves a number of U. S. born citizens who are converts to Islam, and allegedly influenced by foreign powers, including al Qaeda and the Taliban. Semi Osman, Imam of a Seattle Mosque was arrested by the FBI in June, 2002. Reports indicated that at the time of his arrest, a related search revealed documents indicating plans to contaminate water supplies. [7] Subsequently, two brothers, one a founder of the Seattle Mosque, were taken into custody as material witnesses. On August 28th, one of the brothers, James Ujaama, was indicted on charges "of providing the al Qaeda terrorist network with 'training, facilities, computer services, safe houses, and personnel' as part of a conspiracy to 'destroy property and murder and maim persons located outside the United States.' Ujaama, is also accused trying to set up a 'jihad training camp' in rural Oregon in 1999 and of leading discussions there and in Seattle about the need 'to attend violent jihad training camps in Afghanistan.'

The indictment alleged that Ujaama talked about how to poison an unsuspecting public, commit armed robberies, build underground bunkers to hide weapons and firebomb cars." The reports indicate that at the time of his original arrest Ujaama had in his possession documents regarding the poisoning of water.[7] The Fox News report also indicates that information regarding the poisoning of water was likely supplied by Sheikh Abu Hamza Al-Masri. Al-Masri is a one-eyed mullah who is often seen preaching at Finsbury Park's North London Central Mosque and is wanted in Yemen on terrorism charges. Al-Masri is characterized as a radical cleric "suspected of being a major al Qaeda recruiter, according to FBI documents." The articles indicate that members of the mosque were very much under the influence of Al-Masri.

Beyond the contamination possibilities, there have also been open source reports indicating that the terrorist organization al Qaeda has examined the possibility of attacking water retention structures and disrupting water supplies by attacking SCADA systems. On January 29, 2002, the FBI's National Infrastructure Protection Center issued an alert, which states in part, "A computer that belonged to an individual with indirect links to Osama Bin Laden contained structural architecture computer programs that suggested the individual was interested in structural engineering as it related to dams and other water-retaining structures. The computer programs included CATIGE, BEAM, Autocad 2000 and MICROSTRAN, as well as programs used to identify and classify soils using the Unified Soil Classification System."

"In addition, US law enforcement and intelligence agencies have received indications that al Qaeda members have sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA-related Web sites. They specifically sought information on water supply and wastewater management practices in the US and abroad. There has also been interest in insecticides and pest control products at several Web sites."

Interestingly, the last sentence of the FBI alert may be yet another indication of interest in water contamination.

Clearly the pairing of the disruption of water service with the starting of fires would wreak havoc and cause untold loss of life and property, a point made in a recent edition of U. S. News and World Report. It appears that, this too has been considered by al Qaeda.

On September 20, 2002, the Los Angeles Times reported that the recently arrested terrorist cells operated by Omar Faruq in Indonesia had plotted a series of bombings. The report goes on to state "Evidence found in the homes of three suspects included photos of potential targets, hand-drawn diagrams and notes. In addition to the airport and Defense Ministry building, one possible target was the pipeline from Malaysia to Singapore that provides much of the city's water." [8] The article characterizes Faruq stating: "Omar Faruq, an Iraqi captured in Indonesia and quietly handed over to the United States, confessed that

he was al Qaeda's top operative in Southeast Asia and that he plotted to assassinate Indonesian President Megawati Sukarnoputri, according to a confidential U.S. summary of his interrogation. He admits being the mastermind of a series of deadly bombings in Indonesia carried out with the help of Jemaah Islamiah operatives."

Based on the reports cited above, it is evident that interest in poisoning or attacking water systems in some other way is a tactic that has been examined, and likely tried by al Qaeda and related terrorist organizations. The capabilities of such groups in terms of weapons, funding, skills and knowledge remains largely unknown, as they are clandestine terrorist organizations. They do, however, have an established history of attacks that speaks clearly to these issues. Inasmuch as they have repeatedly conducted successful attacks against U. S. entities and interests, both in the U. S. (two attacks on the World Trade Center and one plot to detonate explosives in tunnels and buildings in New York City), and abroad[9] it must be presumed that obtaining weapons, funding and knowledge are not insurmountable issues for these groups. Their record speaks for itself, and tells us that we cannot dismiss this threat. Although no information currently exists to indicate that the facilities of any specific water utility has been targeted by these groups, it is very unlikely that such information will come to light prior to an event, given that these are clandestine organizations.

C. THE NEW THREAT TO WATER INFRASTRUCTURE SECURITY

Water systems can be described in terms of physical components, network attributes, and operational characteristics. Each of these characteristics can be described further in terms of criticality (importance to the system) and vulnerability (ease of contamination or disruption). The contamination or disruption of critical components could yield catastrophic results, such as loss of water supply, system shutdown and toxic contamination. Consequently, vulnerability assessment planning is necessary to assess system security and risk exposure in order to develop a plan that will remove or greatly reduce that risk.

Damage caused can be physical or operational in nature including disruption or destruction of an operating plant or distribution system component, the power supply or other interdependent infrastructure, such as telecommunications, water treatment process, chemical storage containers, particularly chlorine, supervisory control and data acquisition (SCADA) systems, raw water reservoirs, aqueducts, and pumping stations. Utilities must be prepared to deal with any act of intentional damage but the potential for conventional damage to be inflicted on a water supply is much higher than a contamination event. This is not to say that a contamination event is not within the range of possibilities for terrorists.

Of the many known biological warfare agents, nearly all are designed to inflict casualties via inhalation. While less effective as potable water threats, many are capable of inflicting heavy casualties when ingested. Most contaminants would require very large quantities; thereby minimizing an actual threat, leading many to believe the threat of contamination of drinking water through terrorist activities is small. However, in light of the tragic events of September 11, 2001, the ability or desire of terrorists, like al Qaeda, or other vandals with ill-intent to threaten potable water systems should not be underestimated.

D. IS YOUR WATER SUPPLY VULNERABLE TO A TERRORIST ATTACK BY AL QAEDA OR OTHERS?

[10]All U.S. water supplies are potential targets for a terrorist attack. In testimony before a House of Representatives subcommittee on October 11, 2001 Mr. Ronald Dick, director of the Federal Bureau of Investigation's (FBI's) National Infrastructure Protection Center stated that "…water supplies are a logical target for a possible terrorist attack. It is important to note that at this time authorities know of no credible threat to poison any of the nation's drinking water. This is because carrying out such an attack

would be difficult, as the terrorist would need large amounts of a contaminant and knowledge of (and access to) key locations in the water supply and system to introduce the poison." Despite this, the FBI further states that "…all water systems must consider the possibility of a terrorist turning any water supply into a weapon of mass destruction through contamination." The FBI considers such contamination attacks possible, but not probable.

Is your water supply vulnerable to a terrorist attack? That is a question which each water utility must ask itself in this post 9/11 - world that we live in. Prior to September 2001 security was something that was taken for granted and often lightly enforced. Water plants were relatively easy to enter, gates were often left open and access to key facilities was not a problem. Since the events of last fall, however, we have all become more aware of precautions that we must take and the consequences of not acting at all.

We often ask, "…even if a terrorist were to decide to attack a water utility why would he pick mine? If great of damage is desired then why not attack some place more high profile and with a larger population? They would obviously be a better target and create more effect?" We talk ourselves into believing that this could never happen to us so why bother with all of these precautions. It is our lack of concern that has placed these concerns on a slow track and convinced ourselves that such incidences will occur in places far away.

US utilities reacted with an initial increase in security after 9/11/01 by installing security cameras and locking doors, attending seminars and hiring additional security personnel but things have eased up a bit since then. [11]"They've fallen into the regulation trap," said McClure. "Unless the government regulates it, they're not yet taking [security] seriously." "It doesn't matter whether it's al Qaeda or a nation-state or the teenage kid up the street," he said. "Who does the damage to you is far less important than the fact that damage can be done.

The truth of the matter is, however, that terrorism is very real and actually comes from both internal and external threats. Internal threats are sometimes overlooked yet are important to recognize during the implementation of a vulnerability assessment. External threats like al Qaeda are something that is new to us now. We are poised against a nebulus enemy who is neither a state nor a fixed organization against whom we can organize a successful war. We are thus relegated to taking certain precautions and implementing specific security measures that, although do not protect us against every sort of attack, do in fact protect us against the worst of these. It is by taking these precautions that we, in fact, protect our utility.

By hardening our utility we let some other utility become the "softest target in the neighborhood". Terrorists, like anyone else, will take the easiest path to achieve their goals and attacking the easiest/softest target in the most straightforward manner is the path that they have been known to prefer. Al Qaeda, in particular has a track record of using simple but proven methods to create chaos and terror. This, however, is actually good news for us because if we implement even the most minimal basic security measures and procedures into our utility then most likely we become an unattractive target for terrorists. They simply go somewhere else.

Terrorism relies on the fear factor, however. If a terrorist were to poison even one water utility anywhere in the US, no matter how large or how small, fear would be created and, the chaos that would ensue would be for them a large achievement. Since [12] there are approximately 168,000 public water systems in the United States, some serving 8 million people and some serving only 25 people the number of water utility targets open to a terrorist organization is enormous. Unless all of these utilities take security seriously and implement organized security measures then even one incident at a water utility anywhere in the USA could affect us all. Utilities must therefore be on their guard no matter the size, location or perception of insignificance. Activities in the recent past have confirmed the need to make such

preparations and have shown us what al Qaeda and other potential terrorist are actually planning in their terror campaign against the western world. We need to take note at the pattern of events and to prepare accordingly.

E. RECENT TERRORIST ACTIVITIES AGAISNT WATER SUPPLIES & US INFRASTRUCTURE

When it comes to water systems, two types of sabotage need to be considered, vandalism and terrorism. A vandal would interrupt the supply of water and reduce its quantity. A terrorist would contaminate the water and reduce its' quality. It must therefore then be assumed that al Qaeda and other terrorist groups will aim to disrupt the *quality* of our water supplies, something which would affect us both physically and mentally. If they also interrupt the supply of water then they will be pleased with this as well.

Of the various types of potential attacks on the *quality* of water supplies it is much more likely that a biological contamination of the water supply would be attempted because the quantity of contaminant required to impact the system would be less than that needed for chemical contamination. Therefore, the importance of maintaining free chlorine residual in the water distribution system cannot be over-emphasized. Continuous chlorine feed for disinfection is mandatory, not only for regulatory reasons, but also as a method to mitigate the impact of biological warfare against water systems.

A more serious threat to water systems is a physical disruption of service. Disruption of service could result in widespread contamination of a system, and place local communities at risk, for example in the case of fire, as fire flow may not be available to assist in fire fighting activities. Attacks that are designed to disrupt service or render the WTP inoperable are also possible and are much more likely. Consequently, protection measures should be in place at the WTP and ancillary facilities to prevent and protect against both contamination and disruptive (destructive) terrorist actions.

One example of a common ongoing threat is Cryptosporidium, a protozoa excreted in human and animal feces. One such incident occurred in the Milwaukee area[12] in spring 1993 which sickened 400,000 people. Milwaukee was staggered by the nation's largest outbreak of this waterborne disease. Cryptosporidium, a protozoan, passed undetected through two water treatment plants and, once it reached customers' taps, caused more than 400,000 illnesses (mostly diarrhea) and between 50 and 100 deaths out of some 800,000 customers who drank the water.

Cryptosporidium is present in wastewater, and so might have come from a nearby sewage plant; authorities never actually figured out what happened. But a principle was established: pathogens in water supplies can kill. This same principle was known to have been utilized in the second world war to weaken and kill the enemy and could be used as a convenient act of terror at anytime.

Contamination threats can take on various forms, such as in one documented case [13] in North Carolina in 1997 where foam used by firefighters was backed into a neighborhood water supply via a fire hydrant when the fire truck pump was turned on before a safety valve was closed. That incident was accidental but this type of threat could be carried out by a disgruntled employee, a terrorist or some other vandal.

Another incident occurred in [10]Queensland, Australia, on April 23, 2000, when police stopped a car on the road to Deception Bay and found a stolen computer and radio transmitter inside. Using commercially available technology, Vitek Boden, 48, had turned his vehicle into a pirate command center for sewage treatment along Australia's Sunshine Coast.

Boden's arrest solved a mystery that had plagued the Maroochy Shire wastewater system for two months. Somehow the system had been leaking hundreds of thousands of gallons of putrid sludge into parks, rivers and the manicured grounds of the Hyatt Regency hotel. Janelle Bryant of the Australian Environmental Protection Agency said "marine life died, the creek water turned black and the stench was unbearable for residents." Until Boden's capture, during his 46th successful intrusion, the utility's managers did not know why.

Specialists in cyber terrorism have now studied Boden's case because it is the only one known in which someone used a digital control system to deliberately to wreak harm. Details of Boden's intrusion, not disclosed before, show how easily Boden broke in … and actually restrained the power he had. Evidence at trial suggested Boden had quit his job and was angling for a consulting contract to solve the problems he caused.

To sabotage the system he set the system software on his laptop to identify itself as "pumping station 4," then he suppressed all alarms. Paul Chisholm, Hunter Watertech's CEO, said in an interview last week that Boden "was the central control system" during his intrusions, with unlimited command of 300 SCADA nodes governing sewage and drinking water alike. "He could have done anything he liked to the fresh water," Chisholm said.

Like thousands of utilities around the world, Maroochy Shire allowed technicians to remotely operate and manipulate the digital controls. Boden learned how to use those controls as an insider, but the software he used conforms to international standards and manuals he had are available on the web. He faced virtually no obstacles to breaking in. Based on this case and other evidence President Bush has launched a top-priority research program at the Livermore, Sandia and Los Alamos labs to improve safeguards in the estimated three million SCADA systems in use in the US.

[11]In May of 2001, before 9/11, someone else tried to hack into the CAL-Independent System Operator (ISO) site, the nonprofit corporation that controls the distribution of 75 percent of the state of California's power. While the attacker's motives remain unclear, the attacks came while California was in the midst of an energy crisis, and while cities across the state were experiencing rolling blackouts every day. This person or persons was attempting to perform sabotage on the power grid but was never actually successful.

Again just after 9/11, [10]Detective Chris Hsiung of the Mountain View, Calif., police department began investigating a suspicious pattern of surveillance against Silicon Valley computers. From the Middle East and South Asia, unknown browsers were exploring the digital systems used to manage Bay Area utilities and government offices. Hsiung, a specialist in high-technology crime, alerted the FBI's San Francisco computer intrusion squad.

Working with experts at the Lawrence Livermore National Laboratory, the FBI traced back trails of a broader reconnaissance. A forensic summary of the investigation, prepared in the Defense Department, said the bureau found "multiple casings of sites" nationwide. Routed through telecommunications switches in Saudi Arabia, Indonesia and Pakistan, the visitors studied emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities. More information about those devices -- and how to program them -- turned up on al Qaeda computers seized this year, according to law enforcement and national security officials.

Unsettling signs of al Qaeda's aims and skills in cyberspace has led some government experts to conclude that terrorists are at the threshold of using the Internet as a direct instrument of bloodshed. The new threat bears little resemblance to familiar financial disruptions by hackers responsible for viruses and worms. It comes instead at the meeting points between computers and the physical structures they control.

This same type of sabotage could affect a water utility by disabling or taking command of floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, U.S. analysts believe an intruder could use virtual tools to destroy real-world lives and property. They surmise, that with limited evidence, al Qaeda is aiming to employ those techniques in synchrony with "kinetic weapons" such as explosives.

[10]"The event I fear most is a physical attack in conjunction with a successful cyber attack on the responders' 911 system or on the power grid," Ronald Dick, director of the FBI's National Infrastructure Protection Center, told a closed gathering of corporate security executives hosted by Infraguard in Niagara Falls on June 12, 2002.

[10]In an interview, Dick said those additions to a conventional al Qaeda attack might mean that "the first responders couldn't get there ... and water wouldn't flow, and hospitals wouldn't have power thus making the incident many times worse. In Islamic chat rooms, other computers linked to al Qaeda have exhibited access to "cracking" tools used to search out networked computers, scan for security flaws and exploit them to gain entry -- or full command ... al Qaeda prisoners have also described intentions, in general terms, to use those tools to achieve their terrorist aims.

Supervisory Control and Data Acquisition, (SCADA) systems are without a question, vulnerable," said Stuart McClure, president and CTO of security company "Foundstone". For instance, researchers in Finland had identified a serious security hole in the Internet's standard language for routing data through switches. SCADA systems are continuously routing data through such switches. SCADA, systems are ubiquitous at water treatment plants across the country but because the digital controls were not designed with public access in mind, they typically lack even rudimentary security, with fewer safeguards than the purchase of flowers online. SCADA systems are clearly an area of concern.

Computer networks today are critical to water supplies, electric power, natural gas, petroleum protection and distribution, telecommunications, transportation, banking and finance and emergency services. The most alarming terrorist scenario is a combined physical and cyber attack that could bring cascading disruptions on a regional scale. Consequently, a cyber attack could compromise systems monitoring of the water supply, or power sources that run water systems and other vital water system activities.

"We're thinking more in physical terms -- biological agents, isotopes in explosions, other analogies to the fully loaded airplane," he said. "That's more what I'm worried about. When I think of cyber I think of it as ancillary to one of those." "It's not science fiction," Ross said in an interview. "A cyberattack can be launched with fairly limited resources." "…they would be able to conduct an integrated attack using a combination of physical and cyber resources and get an amplification of consequences." But al Qaeda prefers simple, reliable plans and would not allow the success of a large-scale attack "to be dependent on some sophisticated, tricky cyber thing to work."

Al Qaeda's intentions became clearer when in January 2002 in Kabul U.S. forces found something new. They seized a computer at an al Qaeda office which contained models of a dam, made with structural architecture and engineering software, that enabled the planners to simulate its catastrophic failure. This included programs like Microstran, an advanced tool for analyzing steel and concrete structures and Autocad 2000. Clearly they were studying the possibility of blowing up a dam.

Although to destroy a dam physically would require "tons of explosives," Assistant Attorney General Michael Chertoff said a year ago. To breach it from cyberspace is not out of the question. Before 9/11 in 1998, a 12-year-old hacker, exploring on a lark, broke into the computer system that runs Arizona's Roosevelt Dam. [10]He did not know or care, but federal authorities said he had complete command of the

SCADA system controlling the dam's massive floodgates. Roosevelt Dam holds back as much as 1.5 million acre-feet of water, or 489 trillion gallons. That volume, if released, would theoretically cover the city of Phoenix, down river, to a height of five feet. If a 12 year old boy could accomplish this then so could a determined terrorist.

Again, in mid July 2002 the FBI issued the latest in a series of warnings regarding possible terrorist attacks against American targets. This time the nation's water utilities were told to prepare to defend themselves against possible attacks on pumping stations and pipes that serve its cities and suburbs. The effort comes after the discovery of documents in Afghanistan, which indicate that al Qaeda terrorists have been investigating ways to disrupt the U.S. water supply on a massive scale. We have been more alert to security measures following that warning. The al Qaeda threat is real and so their actions must be protected against.

F. WHAT AGENTS MOST LIKELY TO BE USED IN AN ATTACK ON POTABLE WATER SYSTEMS?

[14]Officials in the nation's cities named biological and chemical cyberterrorism at the top of their list of concerns in a survey taken for the anniversary of September's terrorist acts. One ongoing concern cited by the American Waterworks Association has been the possibility that terrorists could disrupt the flow of water to large communities by destroying dams or reservoirs. [13]After touring a Maryland water-testing lab, EPA Administrator, Christine Whitman said it would likely take truckloads of, say, anthrax, to be introduced to a major water system before it had any chance of doing harm. It is often claimed that anthrax can be neutralized by chlorine treatments. 10 percent chlorine solution is said to kill most anthrax spores.

Ms. Whitman is probably correct though, in concluding that the risk in these circumstances is likely to be low. But the key phrase in the paragraph above is "major water system." What about a much smaller arm of a water system? What are the chances that someone or some group with a basic knowledge of hydraulics and some good maps could gain access to pipes that transport water after it is treated for contaminants to a particular neighborhood? Some water utilities have not ignored this potential threat and have been installing alarms in tunnels and locking up access doors to their pipes.

As drinking water is essential to human life, denying it for any period could cause panic and disrupt society. Supply interruptions include the destruction of, or interference with, reservoir dams, water towers or storage facilities, pumping stations, intakes, valves, treatment plants, the distribution system, or fire hydrants, denying the population drinking water or firefighting protection. Supply interruptions can be caused by any number of acts, including physical destruction, interruption of the supervisory control and data acquisition system, or acts that could reduce the water pressure in a system. Supply interruptions can also occur as an indirect result of contamination.

Much of the public concern is focused on the safety of water reservoirs and treatment plants. But in terms of vulnerabilities, the real danger may be the pipes that carry the water, not facilities that store or purify it. Most reservoirs hold between 3 million and 30 million gallons of water, which would significantly dilute any poison to the point that terrorists would have to release enormous quantities to do serious damage. And most poison would be destroyed when the water is purified at a treatment plant. Chlorination, used in most every municipal system, kills or inactivates viruses as well as bacteria like E. Ccoli and salmonella. Some plants also treat water with ozone, which is more effective n killing protozoa like crypto. In most facilities the water is also filtered. Removing particles larger than 1 micron in size will eliminate threats from anthrax and botulinum spores.

Also likely is a truck bomb or another explosive device set off beneath a pumping station, according to Tom Curtis, an executive of the American Water Works Association, whose member utilities supply water to 80 percent of the U.S. population. “For instance,” said Curtis, “one city has six giant pumps, and they’re all in one building. If you crashed an airplane into that building or blew it up, it would cause half a million people to lose their water supply almost instantly. Pumps of this size must be custom-built and can take as long as 18 months to replace.”

Tables 1 and 2 summarize 27 biological warfare agents known or likely to be used in an attack on a potable water system.[15] Among the contaminants shown, some can be inactivated by disinfection process already in place; however, others are resistant or their efficacy is unknown. Additional chemical agents that could be used to contaminate a water supply include sodium cyanide and radioactive materials. Radioactive material, even in minute amounts, could prove to be costly as they would render an entire water distribution system useless.

The eighteen agents shown in Table 1 are infectious agents, eight of which are shown as potable water threats. Based on the ability to weaponize an agent, water threat, infective doses, stability in water and resistance to chlorine, the following list provides a conceptual ranking of those infectious agents that pose a significant threat to potable water, and are ranked in order of increasing to decreasing risk (based on limited data) as:

- Anthrax
- Plague
- Cholera
- Tularemia
- Cryptosporidiosis
- Enteric viruses
- Salmonella
- Shigellosis

Each of the nine biotoxins listed in Table 2 are identified as potable water threats. Of these biotoxins, only botulinum toxins, ricin, staphylococcal enterotoxins, T-2 mycotoxin and possibly alfatoxin are likely to be made available in sufficient quantity to pose a significant potable water threat. Similarly, biotoxins are conceptually ranked as follows:

- Botulinium toxins
- Ricin
- T-2 mycotoxin
- Staphlococcal enterotoxins
- Alflatoxin

G. WHAT ARE THE RELATIVE RISKS TO HEALTH AND WHAT EXPOSURE LEVELS ARE REQUIRED TO CAUSE ILLNESS?

Susceptibility of humans to a particular biological warfare agent is expected to vary widely, especially by age and because of issues related to human immunodeficiency. The values shown in Tables 1 and 2 reflect levels necessary to infect healthy young adults. The infective dose levels for very young, the elderly and immuno-compromised individuals would be somewhat lower. Infective dose estimates shown in Tables 1 and 2 are provided for each biological warfare agent. In the absence of actual data, the ability to quantify infective dose levels is inherently difficult, in most cases limited to extrapolation of rodent

median lethal dose (LD_{50}) values, not to mention that infective dosages are established for inhalation but not ingestion. The numbers are believed to be conservative in that infective doses for ingestion are assumed equal to that by inhalation and infectious agents are accumulated over a seven-day period without discharge from the system.

H. WHERE/HOW ARE THESE SYSTEMS MOST LIKELY TO BE INTRODUCED INTO THE WATER SYSTEM?

The infective dose levels of each biological warfare agent necessitate attacking water supplies closest to the consumer. Consequently, contamination of the raw water supply with a hazardous agent (chemical, biological or radioactive) would most likely not pose a large risk to public health because of the dilution effect, treatment, filtration and disinfection of the water at the existing facilities. Consequently, more critical points in a water system that would be vulnerable to contamination would be at the outlet of the WTP and within the distribution system. These possible attack locations include the clearwell, storage facilities, pump stations, and fire hydrants. Points in the distribution system are very much vulnerable due to their unguarded accessibility and widespread service area. Moreover, every home or building has unprotected access to the distribution system, making detection of contamination extremely difficult. The "bathtub" contamination incident would be nearly impossible to prevent; however, if such a circumstance occurred, this event would only impact a localized portion of the water system. Again, physically destructive actions are more likely to impact the water system than a contamination event.

Personnel associated with the WTP should continue to be diligent in protective security measures, and stay abreast of current events.[16] The staff should routinely keep apprised of industry alerts and utilize the information and data being provided by the United States Environmental Protection Agency and FBI to maintain the highest state of preparedness to protect the water system against terrorist acts. This would include routine reviews of appropriate web sites for updated information on terrorist threats and corresponding plans of action.

I . POSSIBLE SOLUTIONS TO THE THREAT

a. Guard against unplanned and/or unauthorized physical intrusion. Lock all doors, set alarms and provide security at all pumping facilities, vaults and the WTP. Limit access to all facilities and control access to pumping stations, chemical and fuel storage areas, giving close scrutiny to visitors and contractors. Verify all chemical and component deliveries by checking the manifest log against the driver's identification to authenticate the person responsible for the delivery. Post guard(s) at the treatment plant and post "Employee Only" signs in restricted areas. Secure hatches, metering vaults, and other access points to the distribution system. Increase lighting in parking lots, at storage tanks or other areas with limited staffing. Control access to computer networks and control systems, changing passwords frequently. Secure and account for all vehicular and equipment keys; do not leave keys in equipment or vehicles at any time.

b. Review existing emergency response plans to ensure that they are current and relevant to water plant security. Make sure employees have necessary training in emergency operational procedures for response to potential terrorist activities. Develop clear protocols and chain-of-command for reporting and responding to threats along with relevant emergency management, law enforcement, environmental, public health officials, consumers and the media. Ensure key personnel (both on duty and off duty) have access to crucial telephone number and contact information at all times, keeping the call list up to date and easily accessible. Report to local health officials any illness among the employees that might be associated with a water contamination incident. Take mitigating actions to

protect those affected as well as protection from cross-contamination of others (if contagious agent is used).

c. Install access control systems in concentric layers around and within their facilities. Perimeter, building, and office levels. In the outermost ring of protection, boundary components typically include fencing, bollards (short posts or barriers that delimit an area), lighting, signage, guard booths, intercoms, and motorized operators that raise traffic control arms or retract gates on demand.

d. Fire Department requires stations where an electric switch is activated by a key. Irvine, CA and Irving, TX both mandate the installation of a transmitter-receiver system with an effective range of at least 100 ft on all electromechanically controlled gates.

e. By contrast, water utility officials across the country are taking steps to prevent terrorists from reversing the flow of water into a home or business – which can be accomplished with a vacuum cleaner or bicycle pump – and using the resulting "backflow" to push poisons into a local water distribution system. Such an attack would use utility pipes for the opposite of their intended purpose: instead of carrying water out of a tap, the pipes would spread toxins to nearby homes or businesses.

f. All facilities (treatment plants, reservoirs, reservoir dams, water storage facilities and tower, pumping stations, water intake facilities, chlorine booster stations, and meter and valve boxes) should be fenced, be well lighted, and have a perimeter that is monitored by surveillance cameras and motion detectors.

g. To prevent hacking, supervisory control and data acquisition systems for monitoring and controlling water parameters should **not** be connected to the Internet. Remaining cyber security should be enhanced, and passwords should be changed regularly. Industrial facilities are monitored by Supervisory Control and Data Acquisition (SCADA) systems. These systems are often lacking the memory and bandwidth for sophisticated password or authentication systems. SCADA typically runs on DOS, VMS, and Unix platforms, although vendors are now shipping Windows NT and Linux versions, as well.

h. The EPA is considering giving grants to cities to ensure fire hydrants and other entry points to the distribution system are tamperproof. Surveillance cameras should be located on-site at key points, such as at the chlorine storage facilities, chlorine injection areas, filter beds, hazardous chemical and fuel storage areas, and finished water storage areas.

i. By contrast, water utility officials across the country are taking steps to prevent terrorists from reversing the flow of water into a home or business – which can be accomplished with a vacuum cleaner or bicycle pump – and using the resulting "backflow" to push poisons into a local water distribution system. Such an attack would use utility pipes for the opposite of their intended purpose: instead of carrying water out of a tap, the pipes would spread toxins to nearby homes or businesses.

The threat to water utilities in the US from terrorist organizations, such as al Qaeda is very real. Our continual vigilance is needed in order to prevent any harm to our facilities.

Table 1. Summary of threat potential of infectious agents [15]

Agent/Disease	Weaponized	Water Threat	Infective-dose	Stable in Water	Chlorine Tolerance
Anthrax	Yes	Yes	6000 spores (inh)	2 years	Spores resistant
Brucellosis	Yes	Probable	10,000 org. (unk)	20-72 days	Unknown
Cholera	Unknown	Yes	1,000 org. (inh)	Survives well	Easily killed
Clostridium perfringes	Probable	Probable	10^8 org. (inj)	Common in sewage	Resistant
Glanders	Probable	Unlikely	$3.2x10^6$ org. (unk)	Up to 30 days	Unknown
Meliodosis	Possible	Unlikely	Unknown	Unknown	Unknown
Plague	Probable	Yes	500 org. (inh)	16 days	Unknown
Psittacosis	Possible	Possible	Unknown	18-24 hr, seawater	Unknown
Q fever	Yes	Possible	25 org. (unk)	Unknown	Unknown
Salmonella	Unknown	Yes	10^4 org. (inj)	8 days, fresh water	Inactivated
Shigellosis	Unknown	Yes	10^4 org. (inj)	2-3 days	Inactivated, 0.05 ppm, 10 min.
Tularemia	Yes	Yes	10^8 org. (inj)	Up to 90 days	Inactivated, 1 ppm, 5 min.
Typhus	Probable	Unlikely	10 org. (unk)	Unknown	Unknown
Encephalomyelitus	Probable	Unlikely	25 particles (aer)	Unknown	Unknown
Enteric viruses	Unknown	Yes	6 particles (inj)	8-32 days	Readily inactivated (rotavirus)
Hemorrahagic fever	Probable	Unlikely	10^5 particles (inj)	Unknown	Unknown
Smallpox	Possible	Possible	10 particles (uns)	Unknown	Unknown
Cryptosporidiosis	Unknown	Yes	132 oocysts (inj)	Stable days or more	Resistant

Abbreviations: aer = aerosol; inj = injestion; inh = inhalation; unk = unknown.
[1] Total infective dose used to calculate water values.
[2] Ambient temperature, <1ppm free available chlorine, 30 min or as indicated.

Table 2. Summary of threat potential of biotoxins [15]

Agent/Disease	Weaponized	Water Threat	NOAEL, 2 L/day [1]	Stable in Water	Chlorine Tolerance [2]
Aflatoxin	Yes	Yes	75 μg/L	Probably stable	Probably tolerant
Anatoxin A	Unknown	Probable	Unknown	Inactivated in days	Probably tolerant
Botulinum toxins	Yes	Yes	0.0004 μg/L	Stable	Inactivated, 6 ppm, 20 min
Microsystins	Possible	Yes	1.0 μg/L	Probably stable	Resistant at 100 ppm
Ricin	Yes	Yes	15 μg/L	Stable	Resistant at 10 ppm
Saxitoxin	Possible	Yes	0.4 μg/L	Stable	Resistant at 10 ppm
Staphylococcal enterotoxins	Possible	Yes	0.1 μg/L	Probably stable	Unknown
T-2 mycotoxin	Possible	Yes	65 μg/L	Stable	Resistant
Tetrodotoxin	Possible	Yes	1 μg/L	Probably stable	Inactivated, 50 ppm

Abbreviations: NOAEL, no-observed-adverse-effect-level.
[1] Estimated as 7.5 times the NOAEL calculated for consumption of 15 L/day.
[2] Ambient temperature, <1ppm free available chlorine, 30 min or as indicated.

Additional Sources of Information

- EPA Counter-terrorism: http://www.epa.gov/ebtpages/ecounterterrorism.html
- EPA Alert on Chemical Accident Prevention and Site Security: http://www.epa.gov/ceppo/pubs/secale.pdf
- Association of Metropolitan Water Agencies: http://www.amwa.net/isac/amwacip.html
- The International Association of Professional Security Consultants, www.IAPSC.org
- *Protection, Security and Safeguards – Practical Approaches and Perspectives* by Dale L. June, CRC Press, New York, NY, copyright 2000, ISBN: 0-8493-0093-2.
- *Transnational Crime and Terrorism and its Effects on the Maritime Industry*, London, Spring 2001 - Port Technology International
- *Bin Laden: The Man Who Declared War on America;* Yossef Bodansky; 1999 - Prima Publishing
- *Jihad – The Rise of Militant Islam in Central Asia;* Ahmed Rashid; 2000 -Yale University Publishing
- *The New Jackals – Ramzi Yousef, Osama Bin Laden and The Future of Terrorism;* Simon Reeve; 1999 - Northeastern University Press

---

References:

1. Italian police foil alleged cyanide attack on Rome By John Eldridge and Nick Brown
   More information on Jane's Chem-Bio Handbook

2. Ninth arrest in Rome tunnel probe ://www.cnn.com/2002/US/02/25/italy.arrests

3. Cyanide plot to poison Rome water by Bruce Johnston in Rome, Ben Fenton in Washington and Sean O'Neill (Filed: 21/02/2002) Copyright of Telegraph Group Limited 2002

4. Police in Rome have arrested four Moroccans, Radio Netherlands

5. Associate of two suspects sought info on water system
   By Associated Press 10/6/01

6. 6 Men Charged in 9/11 Inquiry
   Copyright 2002 Los Angeles Times

7. Feds Arrest Al Qaeda Suspects With Plans to Poison Water Supplies
   FOX News, Tuesday, July 30, 2002

8. L.A. Times, 2/20/02 - Singapore Cells' Aim Was Jihad
   Probe: Islamists arrested last month planned to ignite a regional holy war, investigators say.

9. Dating from 1983 when Hezbolla repeatedly attacked U. S. facilities in Lebanon to more recent events such as the bombing of U. S. Embassies in Dar al Salaam, Tanzania and Nairobi, Kenya; the bombing of the USS Cole, and in June, 2002, an attempted car bombing of the U. S. Consulate in Karachi, Pakistan, reportedly carried out by a splinter of Harkat Mujahedeen.

10. *US Fears Al Qaeda Cyber Attacks*; by Barry Gellman, June 26, 2002 - Washington Post

11. *Cyberterrorists Don't Care About Your PC*; by Robert Vamosi, ZDNet Reviews, 10 July 2002

12. *Securing US Water Supplies*; by David Isenberg, Center for Defense Information, Terrorism Project, July 19, 2002 - Washington, D.C.

13. *In Over Our Heads? Questions on Protecting US Water Supplies*; by Nicholas Regush, October 25, 2001 - ABC News.com

14. *Cities Name Top Terrorism Concerns*; by Bill Lester, September 4, 2002, Associated Press

15. *Biological Warfare Agents as Threats to Potable Water*; by W. Dickinson Burrows and Sara E. Renner; US Army Center for Health Promotion and Preventative Medicine, Environmental Health Perspectives, Volume 107, Number 12, December 1999; Aberdeen Proving Ground, Maryland

16. *Security of Public Water Supplies*; by R.A. Deininger, P. Literathy and J. Bartram, Environment - Volume 66, 2000, Kluwer Academic Publishers