Second Edition

WEAPONS *of* MASS DESTRUCTION

and TERRORISM

James J.F. Forest
University of Massachusetts, Lowell

Russell D. Howard
Brigadier General USA (Ret.)

Foreword by
Ambassador Michael Sheehan

John McNabb

Chemical and Biological Threats against Public Water Systems[1]

Water is essential for all forms of life, but it is also scarce and vulnerable. While roughly 71 percent of the Earth is covered by water, only 2.5 percent of it is fresh drinkable water; the rest is salt water in the oceans.[2] Further, a significant proportion of fresh water is trapped in glaciers and snow cover. Overall, water is a scarce commodity—less than 1 percent of the Earth's water is fresh water that is available to its nearly 7 billion people.[3] By some estimates, 1.1 billion people in the developing world do not have access to clean drinking water,[4] and this reduces food production, stifles economic growth, and leads to widespread disease and death.[5] In the United States and other developed countries, industrial pollution, stormwater runoff, waste disposal, and development pressures contaminate drinking water supplies. For example, over 100 public water supply wells or wellfields have been closed in Massachusetts[6] from 1960–1985 due to contamination.

Clearly, human survival depends on our ability to protect this vital resource. Drinking water is widely viewed as a "critical infrastructure,"[7] but it is also important to note that private companies are increasingly acquiring drinking water resources and infrastructure which were previously publicly owned. This worldwide trend of increased privatization, according to critics[8], leads to higher water prices, increased stress on water resources, and loss of democratic control over water resources. Today, water is a $400 billion global industry,[9] and some have called it "the new oil."

The U.S. has some of the cleanest, safest drinking water in the world. It has been decades since the U.S. has seen any outbreaks of cholera, dysentery, or other diseases from contaminated drinking water that still occur in other parts of the world. A survey[10] conducted in 2010 by the engineering firm ITT found that 95 percent of American voters value water over any other service they receive, including heat and electricity, nearly one in four American voters is "very concerned" about the state of the nation's water infrastructure, 29 percent of voters agree that water pipes and systems in America are crumbling and approaching a state of crisis, 80 percent of voters say water infrastructure needs reform; and about 40 percent say major reform is needed.

This chapter will describe how public water systems are vulnerable to attack from chemical and biological threats and through their control systems. While history shows that massive deaths from such attacks are difficult to accomplish, such attacks still have occurred throughout thousands of years of recorded human history and continue to this day. A successful attack on one or more public water system would have catastrophic effects on public health and the economy. While some progress has been made since 9/11 to better secure United States drinking water resources, significant vulnerabilities remain which could be exploited by al Qaeda or other attackers.

Intentional Contamination of Water Systems

Drinking water has been the target of attacks for thousands of years.[11] Human history contains a long list of attacks against drinking water, including:

- 500 BC: Assyrians poisoned the wells of their enemies with rye argot.
- 590–650 BC: Athenians threw roots of helleborus into a small river leading from the Pleistrus River to Cirrha during a siege. The enemy forces became violently ill and were defeated.
- 1462: Vlad the Impaler burned villages and poisoned his own wells to deny them to the invading Turks.
- 1939–1942: Japan's Unit 731 poisoned wells and reservoirs in Manchuria with typhoid and other pathogens.
- 1945: Germans polluted a large reservoir in northwestern Bohemia with sewage.
- 1992: In Turkey, potassium cyanide was found in Turkish Air Force water; the Turkish Workers Party, a terrorist group, claimed responsibility.
- 1998–1999: In Kosovo, Serbs disposed of bodies in wells to poison them.
- 2006: In Sri Lanka, Tamil Tiger rebels cut the water supply for government-held villages; the government then attacked the reservoirs.

Homegrown Terrorist Attacks

U.S. drinking water supplies have also been attacked, including by homegrown terrorists and others.[12] For example:

- 1844: A mob destroyed a reservoir in Mercer County, Ohio, that they considered a health hazard.
- 1907–1913: A Los Angeles aqueduct was repeatedly bombed to prevent the diversion of water from Owens Valley to Los Angeles.
- 1972: Two members of the militant cult "Order of the Rising Sun" were arrested in Chicago with botulism, meningitis, anthrax and 30–40 kg of typhoid cultures which they intended to use for poisoning water supplies in Chicago, St. Louis, and other cities.
- 1977: A North Carolina reservoir was contaminated with an unknown poison chemical, shutting down the reservoir.
- 1980: In Pittsburgh, water mains were contaminated with a weedkiller.
- 1984: Members of the Rajneesh religious cult planned to contaminate the Dalles, Oregon city water storage tank with Salmonella, but instead they contaminated salad bars in restaurants, causing an outbreak of 751 cases of Salmonella poisoning.[13]
- 1985: Federal officials learned of a plot by the survivalist group The Covenant, Sword and the Arm of the Lord to contaminate the water supplies of Chicago, New York City and Washington, D.C., with a 30 gallon drum of potassium cyanide.[14]

- 2003: In Greenville, North Carolina, ricin was found at a U.S. Postal Service office with a written note threatening to poison the local water supply.
- 2003: In Michigan, four incendiary devices were found in a water bottling plant; the Environmental Liberation Front (ELF) claimed responsibility.

Al Qaeda's Intentions to Poison Drinking Water

There have also been several indications of al Qaeda's interest in poisoning drinking water. For example, a February 1995 letter by al Qaeda operative Ramzi Youssef, the leader of the group that attacked the World Trade Center in 1993, contained a reference to poisoning drinking water: "We also have the ability to make and use chemicals and poisonous gas for use against vital institutions and residential populations and drinking water sources and others."[15] Other examples include:

- Documents seized by U.S. forces in 2001 at the Tarnak Farms al Qaeda training camp near Kandahar, Afghanistan, showed plans to poison U.S. drinking water and food supplies with pathogens.[16] The seized documents included biological warfare books, manuals, letters, tutorials, fermenter photos, notes and other information, indicating that the group had an active program to acquire biowarfare agents and that they had sought cultures of the following pathogens: B. anthrax, Salmonella typhi, S. paratyphi, Y. pestis, N. miningitus, B. mallei, Cl. Diptheria, CL. Botulinum, B. abortus, and E. coli.[17]
- In his 2002 State of the Union Address, President Bush said that the confiscated al Qaeda documents in Afghanistan included maps of public water systems. "We have found diagrams of American nuclear power plants and public water facilities, detailed instructions for making chemical weapons, surveillance maps of American cities, and thorough descriptions of landmarks in America and throughout the world."[18]
- In early 2002, the FBI arrested two al Qaeda-connected individuals in the United States with documents in their possession about poisoning U.S. drinking water supplies. Then, on January 29, 2002, the National Infrastructure Protection Center issued a bulletin ("Terrorist Interest in Water Supply and SCADA Systems" - Information Bulletin 02-001) which described how "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. In addition, U.S. 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 websites. They specifically sought information on water supply and wastewater management practices in the United States and abroad."[19]
- In February, 2002, Italian police uncovered what appeared to be a plot to poison the water of the U.S. Embassy in Rome with cyanide. According to one media report, "Italian police found approximately ten pounds of a chemical compound containing

italic?

JM: yes

delete?

JM: yes

cyanide in an apartment in Rome with maps highlighting the U.S. embassy and showing the city's water system. When police discovered recently made holes in the underground passageways near the embassy, it looked like a serious threat had been uncovered. However, press reports soon cited officials saying the chemical likely would have become harmless once diluted by the water. Nine Moroccans were arrested, but in April 2004, all were acquitted."[20]

- In 2003, Pakistani authorities arrested Majid Khan, a Pakistani national who was a legal resident of the U.S., and charged him with plotting to poison U.S. drinking water reservoirs, bomb gas stations, and conduct other terrorist acts for Al Qaeda. Khan, who has denied the charges, is being held in Guantanamo.[21]
- In September 2003, the FBI warned that terrorists might use two naturally occurring toxins, nicotine and solanine, to poison U.S. food or water supplies.[22] Nicotine is found in tobacco plants. Solanine—a toxic alkaloid—is found in nightshade, eggplant, and green peppers, among other plants and vegetables. According to an Associate Press report, this FBI bulletin details how "terrorist manuals and documents recovered at Al Qaeda sites in Afghanistan contain references to use of both substances as poisons."[23]
- Documents found in Osama bin Laden's compound in May, 2011, according to ABC News, referenced various plots "to attack infrastructure targets such as water supply and transportation including rail and air . . . In the past, al Qaeda planned for attacks on water supplies have included an interest in mining dams and in poisoning water supply."[24]
- An al Qaeda member was arrested in Spain in August 2011 for threatening to poison the water supplies of tourists to avenge Bin Laden's death and also called for such attacks to be made in Europe and the United States. It was also reported that the suspect "had gone so far as to obtain manuals on poisons, toxins and explosives on jihadist websites."[25]

These and other instances demonstrate an ongoing commitment among al Qaeda members to attack public drinking water systems in the United States and elsewhere. It is thus vital for homeland security professionals to recognize the various ways in which these systems are vulnerable.

Physical Infrastructure Vulnerabilities

Fundamentally, the infrastructure of a local public water system, consisting of open reservoirs, wellfields, treatments plants, pump stations, and hundreds or thousands of miles of distribution water mains with fire hydrants, is impossible to fully secure. An attack on the entire national drinking water physical infrastructure at once is unlikely, highly improbable, if not impossible, because of the fragmented[26] nature of the infrastructure. Unlike the inherently interconnected electrical infrastructure, where a fault or attack on one-two nodes could bring down an entire grid,[27] water utilities are separate entities that would have to be attacked one by one. Therefore the most hardened facilities would be the ones less likely to be attacked.

Another consideration is that each water utility is designed differently: each one is based on specific local requirements based on water quality, location of water resources, growth of the served community over time, and other factors.[28] They vary greatly in size, from serving 25 persons at a time to many millions. There are over 160,000[29] separate drinking water systems in the United States—about 55,000 are community water systems and the rest are very small systems that serve either a small number of people all the time or serve a transient population. While many have emergency interconnections to use for back-up water in case of emergency, and some share water supplies, for the most part an attack on one water system does not threaten any of the others. There has been some consolidation in the U.S. water infrastructure, in the form of water companies that span multiple states. American Water, the largest, serves 16 million people[30] in 1,600 communities and 35 states. Their water facilities, however, are not physically connected, but their facilities are served by the same computer network for administrative purposes. The other water conglomerates include Aquarion Water and U.S. Water.

However, since about 90 percent of U.S. water utilities use chlorine for disinfection, that near universal use of chlorine could serve as a potential Achilles Heel.[31] About 38 percent of chlorine is produced in coastal Louisiana and is transported by rail from there across the United States.[32] An adversary could therefore disrupt a significant portion of U.S. drinking water production by attacking those chlorine plants or the rail lines they use. A less likely but not impossible scenario is that if an adversary could contaminate a significant amount of this chlorine with a radioactive substance,[33] then a significant number of U.S. citizens could be poisoned all at once through this attack vector.

Another important factor to consider is that the physical infrastructure of the national drinking water system[34] is crumbling. Decades of deferred maintenance have left the country with thousands of miles of decaying 100-year-old water mains, clogged distribution systems prone to frequent water main breaks, substandard and failing treatment plants, broken and unusable fire hydrants, and insufficient storage capacity to provide fire protection. The American Society of Civil Engineers gives the nation's drinking water infrastructure a D- grade and estimates that an investment of at least $220 billion[35] over the next 20 years is needed.

Water System Components

A drinking water utility is composed of four primary physical components: supply, treatment, storage, and distribution:

- Water Supply. The source of the public water supply is from groundwater or surface water. Groundwater is contained in an underwater reservoir or river called an "aquifer" which is collected by pumping the water to the surface in a well or well field. Surface water sources can be a natural body of water, such as a river, pond, or lake, or an artificial body of water called a "reservoir" which was created by the impoundment of water by a dam. An aquifer can be contaminated by direct injection of pollutants into the well or into the aquifer, by leaking underground storage tanks, or by runoff of pollutants into the surface area above an aquifer, the area closest to the well being the most vulnerable. A surface water source can be contaminated by direct dumping of pollutants into the water body or by runoff of pollutants into the watershed area which drains into the water body.

- Water Treatment. Typical treatment includes an intake of the source water, flocculation/sedimentation to take out relatively large solid matter, addition of alum to control pH, filtration to take out smaller solid matter, oxidation or ion exchange to consume dissolved organic matter, reverse osmosis, ozonozation, and chlorination to disinfect the water. The concentration of each of the treatment chemicals added is paced according to the volume and rate of flow into the treatment plant. The quality of the water leaving the plant can be adversely affected by an increase or decrease in the proper amount of treatment chemicals, for example if the chlorination pumps were turned off then the water would not be disinfected and would threaten public health.
- Water Storage. One or more finished water storage tanks are used in a public water supply system to store the unused water that had been pumped from the treatment plant to distribution, and also to provide the required pressure to the distribution system. The pressure is dictated by the difference in elevation from the top of the water in the tank to the elevation of the pipe bringing water into a customer's dwelling. Tanks are typically composed of concrete or steel. Many systems monitor the chlorine residual in the tanks, because if water is allowed to sit too long in a tank the chlorine will decay, allowing the growth of pathogens which could threaten public health.
- Water Distribution. The final step is the delivery of the finished water from the treatment plant to the customer, via water mains and pipes, which are typically made these days of ductile iron or plastic (older pipes were made of cast iron or concrete asbestos). The distribution systems also includes many fire hydrants, blowoffs (to allow flushing at the end of a pipe if there is no hydrant there), valves, and the connections. Over time the water mains can become clogged with accumulated sediment left over from the treatment process, valves can break from years of wear and tear, and hydrants can freeze. The hydrants, blowoffs, and connections are all potential locations for the entrance of contaminants from backflow pressure if the pressure of a contaminated water source, say from a whole building sprinkler system, exceeds the pressure of the distribution system. Backflow preventers are usually required to be installed in such locations.

Actual Contamination Incidents

There are many examples of drinking water in public water systems which have been contaminated unintentionally through each of these components. For example:

- Water Source: In one of the most serious water contamination incidents in North America in recent times, in May 2000, in Walkerton,[36] Ontario, seven people died and hundreds became seriously ill from an E. coli contamination of their groundwater supplies by a massive manure runoff from nearby farms.
- Water Treatment: On July 6, 1988, the inadvertent dumping of 20 tons of aluminum sulphate into the wrong tank at the water treatment plant in Camelford, England,[37] killed at least 20 people and made thousands more very sick with aluminum poisoning.

italic?

JM : yes

italic?

JM: yes

- Water Storage: The City of Woburn, Massachusetts, issued a boil water order[38] in March, 2007 because of animal waste that had gotten into the Rag Rock water storage tanks, contaminating the water with E. coli bacteria. Woburn was also the site of an earlier incident during the 1970s and early '80s, in which the improper disposing of industrial solvents by two corporations was linked to water contamination in the groundwater pumped from wells G and H, contributing to an unusually high number of childhood leukemia cases, cancer and other health problems.
- Water Distribution: The EPA has compiled a list[39] of 459 backflow incidents in water distributions systems in the U.S. that have resulted in 12,093 illnesses from 1970 to 2001. In a backflow incident, contaminated water from inside a building, irrigation system, sprinkler system, etc. is siphoned into the public water system resulting in contamination of the drinking water in the distribution system, leading to illness and public health impacts.

Vulnerability Assessments

Although nothing should be ruled out entirely, the potential vulnerabilities of each component are summarized in Table 1.

Table 1

Vulnerability Assessments of Water System Components

Component	Characteristics	Vulnerability Assessments
Water Supply	• Well fields. The source water is underground and out of sight. • Natural water bodies and reservoirs. The source water is in plain sight, exposed, but there is a large volume of water. • Dams create artificial reservoirs by holding back large volumes of water.	• Cost to monitor reservoir is very high and not 100% effective • Dams could be attacked with conventional explosives to inundate populated areas, but this does not poison drinking water. • Reservoirs have a large volume of water that would require large amount of contaminant to overcome dilution. • Reservoirs are difficult to monitor and impossible to fully protect. • Wells are potentially most vulnerable at the well head where water is pumped out of the aquifer, treated, as pumped to distribution. • Wells could be intentionally contaminated in the area adjacent to the well head where surface water runoff drains into the aquifer, but there is little certainty that this would be effective. Since water goes next to treatment, this reduces this vulnerability. • Retention time of water can be weeks or months, increasing the time for the

		contaminant agent to be further diluted or degraded, and also delays the period between the contamination and its effect. • Well heads are usually enclosed, guarded, and monitored regularly. However, the well heads and pumping stations are usually in remote locations which may not be manned continuously and be monitored only remotely. • **Overall, low risk**
Water Treatment	• Treatment plants are usually in enclosed buildings with fencing, video surveillance, and alarm systems, and are relatively easy to adequately protect. • The most vulnerable point is the clearwell, where finished water is pumped directly to the distribution system. • Each treatment plant is unique.	• Since each plant is unique, any attack would require substantial research & local knowledge to change process to poison water. • There are multiple injection points in a treatment plant that could be vectors of attack. • A conventional sabotage attack with explosives could cripple a treatment plant for weeks or months, especially if the high lift pumps, which in most cases are custom-made, are damaged or destroyed. • Highest potential for risk would be an insider attack. • **Low risk**.
Water Storage	• Finished water storage tanks collect water not used in distribution for use when treatment plant is not running. • These also provide pressure to the system equal to that provided by the plant's high lift pumps.	• Water in tank is after treatment and not tested for more than coliform bacteria, so contaminants unlikely to be detected. • There are very few storage tanks in any system so they are easy to adequately guard. • Access points for elevated tanks are at the top of the tank, limiting the amount of contaminant to what can be carried to the top while avoiding detection. • **Low to Medium risk**.
Water Distribution	• Even a small utility will have dozens of miles of water mains and hundreds of fire hydrants. • Large utilities will have hundreds of miles of water mains and thousands of fire hydrants. • Every connection by a customer to the system is a potential attack vector.	• Water mains and hydrants are usually not fully maintained because of costs. • Impossible to fully protect all water mains and hydrants from attack, too many of them. • Connections are underground and out of sight, and are inside private property. • **Medium to High risk**.

Effective Chemical, Biological and Radiological Agents for Drinking Water Contamination

According to analysis by Peter Gleick, a chemical, biological or radiological (CBR) agent used for contaminating a drinking water supply must have several characteristics, including:

- "Weaponized: it must be produced and disseminated in quantities sufficient to have the intended effect.
- Appropriate for water dissemination: it must be viable, dissolvable, stable and transportable in water.
- Infectious, virulent or toxic: it must be effective at causing illness or death, with no widespread immunity in the target population.
- Effective over time and treatment: it must maintain its effectiveness in water long enough to reach and affect humans and it must not be negated by standard water treatment systems likely to be in place.[40]

As reflected in Table 2, there are a wide variety of CBR agents that meet these criteria and could potentially be used to poison a public drinking water supply: [41]

Table 2

Chemical and Biological Contaminants of Water

Class	Examples (not exhaustive)
Microbiological contaminants	
Bacteria	Bacillus anthracis, Brucella spp., Burkholderia spp., Campylobacter spp., Clostridium perfringens, E. coli O157:H7, Francisella tularensis, Salmonella typhi, Shigella spp., Vibrio cholerae
Viruses	Caliciviruses, Enteroviruses, Hepatitis A/E, Variola
Parasites	Cryptosporidium parvum, Entamoeba histolytica, Toxoplasma gondii
Inorganic chemicals	
Corrosives and caustics	Hydrochloric acid, sulfuric acid, sodium hydroxide
Cyanide salts or cyanogenics	Sodium cyanide, potassium cyanide, amygdalin, cyanogen chloride, ferricyanide salts
Metals	Mercury, lead, osmium, their salts, organic compounds and complexes (even those of iron, cobalt, copper are toxic at high doses)
Non-metal oxyanions, organo non-metals	Arsenate, arsenite, selenite salts, organoarsenic, organoselenium compounds
Organic chemicals	
Fluorinated organics	Sodium trifluoroacetate (a rat poison), fluoroalcohols, fluorinated surfactants

italic?

JM: no x2

italic?

Hydrocarbons and their oxygenated and/or halogenated derivatives	Paint thinners, gasoline, kerosene, ketones, alcohols, ethers (e.g. methyl tert-butyl ether or MTBE), halohydrocarbons (e.g. dichloromethane, tetrachloroethene)
Insecticides	Organophosphates (e.g. Malathion), chlorinated organics (e.g. DDT), carbamates (e.g. Aldicarb) some alkaloids (e.g. nicotine)
Malodorous, noxious, foul-tasting, and/or lachrymatory chemicals	Thiols (e.g. mercaptoacetic acid, mercaptoethanol), amines (e.g. cadaverine, putrescine), inorganic esters (e.g. trimethylphosphite, dimethylsulfate, acrolein)
Organics, water-miscible	Acetone, methanol, ethylene glycol (antifreeze), phenols, Detergents
Pesticides other than insecticides	Herbicides (e.g. chlorophenoxy or atrazine derivatives), rodenticides (e.g. super-warfarins, zinc phosphide, *a*-naphthyl thiourea)
Pharmaceuticals	Cardiac glycosides, some alkaloids, antineoplastic chemotherapies, anticoagulants (e.g. warfarin). Illicit drugs such as LSD, PCP and heroin
Chemical warfare agents	
Chemical weapons	Organophosphate nerve agents (e.g. sarin, tabun, VX), vesicants, [nitrogen and sulfur mustards (chlorinated alkyl amines and thioethers, respectively)], Lewisite
Biotoxins	
Biologically produced toxins	Biotoxins from bacteria, plants, fungi, protists, defensive poisons in some marine or terrestrial animals. Examples include ricin, saxitoxin, botulinum toxins, T-2 mycotoxins, microcystins
Radiological contaminants	
Radionuclides	Does not refer to nuclear weapons. Radionuclides may be used in medical devices and industrial irradiators (cesium-137 iridium-192, cobalt-60, strontium-90).[42] Class includes both metals and salts.

As this table illustrates, acquiring at least one of these is not difficult, and some are more difficult to acquire than others.

The Most Likely Physical Attack Scenario

The most likely attack vector is through the distribution system, which is the most vulnerable[43] component of a public water system. While each component has vulnerabilities, as discussed above, the consensus from a number of studies on this subject is that if the attackers objective is to actually poison and kill the maximum amount of people, and not to

merely threaten to poison the water or to disrupt water delivery, then the attack would be directed through the distribution system.

In one recent study, researchers used a hypothetical "backflow attack" to demonstrate the effects of a CBR agent on a water distribution system. Using this method, pumps such as used by lawn chemical companies are used to inject chemicals (e.g., weed killer or some other item listed in Table 2 above) into the distribution system. The injection point could be any existing connection to the distribution system, such as a fire hydrant or a connection in the basement of a building where the activity would not be immediately detected. The pump used for this type of attack would need to exceed the pressure gradient of the water in the systems water mains, usually around 80 pounds per cubic inch. It is estimated that using this method, a few gallons of a toxic agent could contaminate a system serving around 150,000 people in just a few hours.[44]

According to a similar study published in the January 2005 *Journal of the American Water Works Association,* the attacker would need a detailed knowledge of the hydraulics of the water distribution system, and the most effective method would be to use a slow injection of the contaminants from a connection to a major distribution water main in the distribution system over a long period of time.[45] This method could also be used to target a specific building or facility. With knowledge of the hydraulic conditions in the distribution system, and some calculations, an adversary could inject a relatively small amount of toxin in a fire hydrant near the facility which would result in a lethal dose being received in the water at that location.

To protect against such an attack, the water utility would need a "highly dense system of detectors"[46] in its distribution systems, calibrated to look for general indicators of water quality, such as conductance; such general indicators should be sufficient to detect most forms of contamination that would be injurious to human health (but not all potential agents). Also, as the authors of the 2005 study noted, if fire hydrants are to be located on the main distribution mains they should be equipped with backflow preventers. In essence, the only effective defense against attacks on a water distribution system is continuous real-time monitoring of the quality of the water in the system. There are many such monitoring systems on the market today, but so far very few water utilities have installed them because of the cost and a perceived lack of urgent need for them.

Potential Al Qaeda Attack Scenarios

As noted above, al Qaeda members have repeatedly stated their intention to "poison" the U.S. drinking water supply, and have conducted research and actively worked on developing poisons and means of delivering them. Of all the possible toxins or pathogens they could potentially use, including those found in the Tarnak Farms documents, the one that is the easiest for them to produce is ricin, made from castor beans.

According to the former Director of National Intelligence Dennis Blair in his 2010 Annual Threat Assessment, "if al-Qa'ida develops chemical, biological, radiological, or nuclear (CBRN) capabilities and has operatives trained to use them, it will do so. Counterterrorism actions have dealt a significant blow to al-Qa'ida's near-term efforts to develop a sophisticated CBRN attack capability, although we judge the group is still intent on its acquisition."[47]

Al Qaeda members have shown a particular interest in ricin, a highly toxic biotoxin which is weaponized, appropriate for dissemination in water, and is resistant to chlorination. Ricin is by far not the ideal waterborne poison, but its main advantage is that it is easy to produce. Lesson 16 in the *Al Qaeda Training Manual,*[48] "Assassinations Using Poisons and Cold Steel" provides instructions on how to extract the poison ricin from castor beans. Ricin-making apparatus or traces of Ricin, and manuals with detailed instructions for making and using Ricin, have been found in police raids on al Qaeda cells in Great Britain, France, Spain, Russia, Georgia, Afghanistan, and Kurdish-controlled northern Iraq.[49]

Assuming that al Qaeda still has sufficient manpower and funds to plan and carry out an attack to poison the U.S. drinking water supply, how would they go about it? They would not need to attempt to contaminate the entire water system of a city. Most likely they would use the ricin (or other poison) in a specific targeted backflow attack on a key building or facility which has high symbolic value and which would bring the maximum publicity in addition to as many casualties that they could produce. Government agencies must identify the most likely targets of such an attack, and take the necessary action to secure prime target water supplies by installing backflow prevention devices and real time contaminant monitoring, as well as securing the water supply connections to these facilities. Clearly, al Qaeda has the motivation for mounting such an attack, and is actively seeking the means to do so; they must be prevented from having any opportunity to succeed.

Response to a Water Contamination Incident

The first challenge in responding to a water contamination incident is knowing that an incident is actually occurring. If the contamination was introduced in the distribution system and there is no real-time contaminant monitoring (which is the case in almost all water systems), then the first indication would be one or more people getting sick or dying. That would bring them to the attention of the local doctor or hospital, who may or may not connect the illness with a waterborne disease as opposed to another potential cause such as food poisoning.

According to a recent study, most health care professionals have had limited or no training in medical school or in their subsequent practice in recognizing waterborne diseases.[50] The affected person may or may not recognize the source of their illness as their drinking water. Any delay in recognizing that the illness has been caused by waterborne agents will serve to increase the number of cases, further spread the agent through the water system, and further delay the identification and management of the problem.

The Centers for Disease Control has called on the medical community to remain vigilant, to observe and respond to unusual disease trends, and to detect and control intentional contamination of public drinking water supplies.[51] An online resource[52] for health care workers provides information to help them recognize and manage waterborne diseases from intentional or natural causes. The website also contains information on *Physician Preparedness for Acts of Water Terrorism,* including clinically relevant information on waterborne disease, and special risk communication and patient risk evaluation guidelines.[53]

An intentional contamination of a public water system may be detected first by the water utility, through its water testing or from an obvious security breach; perpetrators of such an attack might also publicly announce the contamination. In such cases, it is clearly

important for the utility to involve the public health community. Both the water utility and the local public health community must work together to identify and effectively respond to the problem; the public health officials to treat the affected residents and the water utility to take appropriate actions to contain and eliminate the contamination.[54]

The United States Environmental Protection Agency (EPA) has prepared a number of guidance documents to help local water utilities respond to drinking water contamination threats and incidents, including:

- A Water Security Handbook: Planning for and Responding to Drinking Water Threats and Incidents[55]
- Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents[56]
- Emergency Response Plan Guidance for Small and Medium Community Water Systems to Comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002[57]

The Cyber Threat Dimension: Water System SCADA Control System Vulnerabilities

Supervisory Control and Data Acquisition (SCADA)[58] is the term usually used to describe the computerized central control system used in many drinking water utilities, as well as in many other industrial, manufacturing, and energy facilities. SCADA replaced the legacy control schemes which utilized electro-mechanical process control.

Historically, drinking water treatment facilities were isolated systems accessible only through physical access to the valves, chemical feed units, and control panel in the water treatment plant. In these legacy control systems, each valve, chemical feeder, and mechanism was connected by individual wires to one or more central control panels where the operator could view the many dials and meters showing the status of each component and could change the settings individually as needed. Remote facilities like water storage tanks, reservoir gates, and pump stations, were also connected through radio, telephone, cable, or other means. However, in the past three decades many water utilities have retrofitted their facilities by installing computer-controlled SCADA or other control system type hardware and software.[59] The dedicated communications channels for remote facilities were in most cases replaced by internet connections,[60] and also in many cases remote operation over the internet of the SCADA system was implemented. A computer screen replaced the large mechanical control panel with its dozens of dials, levers and mechanical registers.

SCADA systems were designed to provide consistent and reliable access; security considerations were not in the forefront of design concerns. A public water system is expected to operate 24 hours a day, every day, setting the flow rate of water entering the plant, automatically setting the amounts of treatment chemicals to keep pace with the flow rate, and timing the flocculation, settling, and filtration phases to meet the required time periods to be effective. As a results, the computer systems that control these actions are not designed to be regularly updated with security patches (which often require a system to pause services or even restart). Many water utility SCADA systems were designed in isolation, but most of this kind of software runs on Microsoft Windows XP or Server 2003 systems.[61]

Some do not have regular internet access, but many do. Both of these factors contribute to the vulnerability of drinking water facilities to intentional or unintentional intrusions.[62]

By 2004, according to a report by the U.S. Government Accountability Office (GAO), industrial control systems in general had become vulnerable because of 1) adoption of standardized technologies with known vulnerabilities, 2) connectivity of control systems with other networks, 3) insecure remote connections, and 4) widespread availability of technical information about control systems.[63] A March 2008 report by the Water Sector Coordinating Council's Cyber Security Working Group, lists a variety of "water sector industrial control system risks today" including design limitations, more open environments, increased connectivity and complexity, system accessibility, supply chain limitations and information availability.[64] This report, *Roadmap to Secure Control Systems in the Water Sector,*[65] states that there are many ways in which a cyber event[66] can affect a water system, "some with potentially significant adverse effects in public health," such as:

- Interfere with the operation of water treatment equipment, which can cause chemical over- or under-dosing
- Make unauthorized changes to programmed instruction in local processors to take control of water distribution or wastewater collection systems, resulting in disabled service, reduced pressure flows of water into fire hydrants, or overflow of untreated sewage into public waterways
- Modify the control systems software, producing unpredictable results
- Block data or send false information to operators to prevent them from being aware of conditions or to initiate inappropriate actions
- Change alarm thresholds or disable them
- Prevent access to account information

Further, the report notes that although many facilities have manual backup procedures in place, the failure of multiple systems at once may overtax staff resources—even if each failure is manageable by itself.

Other reports of note include the *Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats,* by Greylogic (June 2010), which describes how state and/or non-state actors from China, Russia, and Turkey are "almost certainly" targeting and penetrating the networks of energy providers and other critical infrastructure in the United States and other countries, and projects that network attacks on the power grid will escalate over the next 12 months.[67] A 2010 report by McAfee, based on a survey of 600 IT and security executives from critical infrastructures in 14 countries all over the world, indicated that networks and control systems are under repeated cyberattacks, and that the reported cost of downtime from major attacks is more than U.S.$6 million a day.[68] This report also noted that 75 percent of control systems overall are connected to the internet or other IP network, but in the water/wastewater sector only 55 percent are so connected; only 33 percent of critical infrastructure services overall have policies that restrict or ban the use of USB sticks or other removable memory; and that 77 percent of professionals in the water/wastewater sector said that government regulation had either diverted resources from improving security or had no effect.

Another report by McAfee, published in 2011, describes how many IT security executives at critical infrastructure facilities—including water supply facilities—in 14 countries believe that their vulnerability had increased since the previous year, and concludes that "they are not ready" for a cyberattack.[69] In addition, the report noted that 80 percent of the executives said they had been hit with a large-scale Denial of Service (DDos) attack (an increase over the 50 percent reported the previous year); 70 percent said they frequently found dangerous malware on their systems; and 85 percent reported at least one network intrusion. And in 2011 a report by the Department of Homeland Security concluded that in 2011 the most commonly found vulnerabilities in industrial control systems were credentials management, weak firewall rules, and network design weaknesses.[70] These and other documents illustrate how contemporary public water systems are vulnerable to a cyber attack.

Known Water System SCADA Cyber Attacks

There are only a handful of publicly disclosed SCADA cyber attacks involving drinking water and wastewater facilities, including:[71]

- 1994–Salt River Project Water Dept., Arizona; 27-year-old hacker reportedly broke into computers but was never in control of dams[72]
- 2000–Maroochy Water System, Australia; former consultant took control of wireless pump system 46 times to spill 264,000 gallons of raw sewage onto waterways.
- 2006–Harrisburg, Pennsylvania water treatment plant; foreign hacker planted malware in plant computers to use them to distribute spam and pirated software
- 2007–Tehema Colusa Canal Authority, California; former employee remotely installed unauthorized software on a SCADA computer that controlled the flow of water
- 2009–Russian and Chinese spies have infiltrated the U.S. electric grids, mapping the grids and planted bugs that could disrupt them, senior U.S. intelligence officials told the Wall Street Journal.

The Department of Homeland Security publishes a daily Open Source Infrastructure Report[73] which summarizes incidents that often involve public water systems. In 2010, these reports revealed a total of 914 "Water Sector" incidents, including 246 incidents at drinking water treatment facilities. Of these, 71 involved water contamination, 79 were water main breaks, 18 were chlorine leaks, 13 involved plant malfunctions, and 12 were incidents of vandalism. There was only one reported incident of a "terrorist threat," which turned out to be a hoax.[74] Four incidents are of particular interest to this discussion, in that they involved computer systems:

- March 2010: The public water system in Silver City, New Mexico, lost 3 million gallons because of a water leak that investigators linked to a possible malfunction in their newly installed SCADA system.[75]
- June 2010: A computer failure caused the public water plant in Lake Chelan, Washington, to stop operating.[76]
- September 2010: A computer malfunction apparently shut down the water plant in Glidden, Iowa and drained the town's water storage tank.[77]

- December 2010: The water plant in New Canaan, Connecticut, was shut down because of a computer malfunction, but water was still pumped into and through the plant, causing flooding from the plant across the nearby roadway.[78]

Finally, some incidents within the past year have served to heighten concerns over the cyber security of drinking water facilities. In June 2011, an IT security professional performed a penetration test for an unnamed Southern California water utility, and was able to gain control of the utility's chemical control systems in less than a day. The route of exploitation was workers who were able to remote into the SCADA system from home.[79] In August 2011, another IT security professional giving a demonstration a the annual Black Hat IT security conference in Las Vegas showed how to use Google to access the Programmable Logic Controller (PLC) of a water treatment plant pump, but he did not try to remotely have it do anything. And a February 2011 report by McAfee described an event which became known as Operation "Night Dragon,"[80] a "coordinated covert and targeted cyberattacks . . . conducted against global oil, energy and petrochemical companies." The objective appeared to be theft of intellectual property and trade secrets.

But perhaps the most significant development within recent years—in terms of cybersecurity and critical infrastructure—is the Stuxnet worm, the first malware specifically designed to attack SCADA systems. Stuxnet potentially shows the way for a cyber attack on a water treatment plants as well as other infrastructure SCADA systems.

The Powerful Stuxnet Worm

In June, 2010, the IT security world was rocked by the discovery by security firm VirusBlokAda of a powerful worm[81] which was showing up in control systems all over the world. While it was first thought that Stuxnet was designed to steal trade secrets and intellectual property, it was soon learned that even though Stuxnet was found in computers and control systems all over the world, it affected only certain Siemens control systems used for controlling centrifuges in the Iranian nuclear development program. Stuxnet is considered a "game-changer" because it is the first known malware to effectively attack SCADA systems. It utilized four previously unknown vulnerabilities in the Windows operating system used to run the Siemens' control system software—a major accomplishment, since most successful malware tend to exploit just one undiscovered vulnerability. Stuxnet was also designed to successfully bridge the "air gap" supposedly protecting the Siemens systems: in other words, the machines were not connected to the internet, but the worm was still spread by using thumb drives as the delivery method.

In its Stuxnet Dossier, the IT security firm Symantec describes Stuxnet as "a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries."[82] The Dossier also described specific characteristics of Stuxnet, including that it self-replicates through removable drives, exploiting a vulnerability allowing auto-execution; can spread through a vulnerability in the Windows Print Spooler; attempts to bypass security products; contacts a command and control server that allows the hacker to download and execute code, including updated versions; and fingerprints a specific industrial control system and modifies code on the Siemens PLCs to potentially sabotage the system.

While the objective of Stuxnet was apparently to damage the Iranian nuclear program, its methodology could be applied, or its code could be altered, to attack other industrial control systems such as those at a water treatment plant. Of course, it still would take an enormous amount of reconnaissance and research to design a Stuxnet-like malware to attack a water treatment plant, and a separate design may be needed for each individual plant attacked, because of their uniqueness, but it's possible. Perhaps only a nation-state would have the resources to accomplish this (as has been surmised about Stuxnet), but perhaps not. If that day comes, then the question becomes whether the water sector has the capability to defend against an attack from malware delivered through USB drives; right now, the answer to that question is an emphatic "No."

Summary of the Cyber Threat to Public Drinking Water Systems

By spring 2011, about one year after the discovery of Stuxnet, there had been a plethora of additional vulnerabilities discovered in SCADA systems used around the world and in water utilities. The antivirus company Symantec reports[83] that there had been 15 new SCADA vulnerabilities disclosed in 2010, one more than the 14 publicly disclosed vulnerabilities in 2009. In March, 2011, Italian security researcher Luigi Auriemma released proof of concept code on 34 SCADA vulnerabilities to Bugtraq (an online repository of software vulnerabilities), which was followed by many advisories from ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). These vulnerabilities, according to Auriemma,[84] would allow an attacker to execute a program remotely on a SCADA system with an internet connection, allow attackers to access stored data or to interfere with the process control hardware that is run by the SCADA system.

Many other SCADA vulnerabilities have continued to be revealed during 2011. For example, a Russian security firm, Gleg, has offered an exploit pack for SCADA systems called SCADA + with 22 modules incorporating 11 previously unknown vulnerabilities.

There has been speculation that the release of Stuxnet could be followed by some kind of modified "Son-of-Stuxnet", based on the capability shown by the original Stuxnet. Witnesses testifying in a hearing in November 2010 before the Senate Committee on Homeland Security and Government Affairs testified that variants of Stuxnet could be used to attack other critical infrastructure, such as the power grid, transportation systems, or water supplies.[85]

Stuxnet could be leading the way[86] as the first "weaponized" malware, setting a precedent for newer variants targeting different applications because:

(1) Stuxnet provided a "step-by-step cookbook" for SCADA malware design;

(2) There are many vulnerabilities in SCADA that have been discovered since Stuxnet, and many more most likely remain to be discovered;

(3) Specific knowledge of the target process used by the PLC's controlled by the SCADA software isn't necessarily needed; and

(4) The Stuxnet-type code that is now available provides the basic structure to remotely control a SCADA process for whatever objective the attacker might want, the customizations can be added as needed.

Clearly, the United States does face potential cyber attacks, on our critical infrastructure and other assets, from nation states, terrorist networks, criminal groups, malicious hackers, and others, as pointed out by Director of National Intelligence Dennis Blair in his Annual Threat Assessment: "Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication."[87] Almost a decade earlier, the CIA indicated in a Senate hearing that they were alert to the possibility of al Qaeda and Sunni extremists planning cyberwarfare attacks against U.S. critical infrastructures:

> Cyberwarfare attacks against our critical infrastructure systems will become an increasingly viable option for terrorists as they become more familiar with these targets, and the technologies required to attack them. Various terrorist groups—including al-Qa'ida and Hizballah—are becoming more adept at using the Internet and computer technologies, and the FBI is monitoring an increasing number of cyber threats. . . . These groups have both the intentions and the desire to develop some of the cyberskills necessary to forge an effective cyber attack modus operandi.[88]

As noted earlier, there is evidence that al Qaeda has been researching SCADA and control system used in drinking water and wastewater, as previously mentioned. However, most observers conclude that al Qaeda does not have the skills, manpower, or technical sophistication to carry out a cyber attack on critical infrastructure, or any other cyber attack. One reason is that most of their key computer experts have been captured or killed.[89] Dorothy Denning, of the Center on Terrorism and Irregular Warfare at the Naval Postgraduate School, has been closely examining this issue for many years, and recently concluded that "Terrorists have not yet demonstrated that they have the knowledge and skills to conduct highly damaging attacks against critical infrastructures (e.g. causing power outages) although there are a few indicators showing at least some interest . . . At least in the near future, bombs remain a much larger threat than bytes."[90]

Securing the Water Sector

Responsibility for the security, maintenance, and operation of a local water utility is principally the sole responsibility of that utility, subject to applicable local laws & regulations, the state regulatory authorities, and the U.S. Environmental Protection Agency (EPA). Homeland Security Presidential Directive 9 (HSPD9) directed the EPA to develop a surveillance and monitoring program to provide early warning detection of a terrorist attack using biological, chemical or radiological (CBR) weapons:

> The Water Security (WS) initiative is a U.S. Environmental Protection Agency (EPA) program that addresses the risk of contamination of drinking water distribution systems. EPA established this initiative in response to Homeland Security Presidential Directive 9, EPA deployed the first full-scale, comprehensive CWS pilot in partnership with the City of Cincinnati at the Greater Cincinnati Water Works (GCWW). Planning and pre-design activities for the pilot began in December 2005, were substantially completed in June 2009, and data collection concluded in June 2010. The drinking water CWS components are fully operational, with performance data continuing to be evaluated by EPA. EPA awarded funding for CWS pilots in New York City, San Francisco, Philadelphia, and Dallas. These four additional pilots were selected through a national competition and will conclude in 2012.[91]

In addition, the Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188, 42 U.S.C. 300i) amended the Safe Drinking Water Act[92] to require community water systems serving more than 3,300 individuals to complete a vulnerability assessment, prepare an emergency response plan, and to submit them to the EPA. These vulnerability assessments[93] had only one question regarding general PC security (passwords, etc.) and did not address control system security. Furthermore, neither the Bioterrorism Act, nor any other federal law or regulation require any water utility to actually make security upgrades to address vulnerabilities; provide funds to help water utilities to make security improvements; or require water utilities to revise or update the vulnerability assessment or emergency response plan after they were completed in 2003-2004.

The progress of U.S. drinking water systems in improving their overall security was assessed in a talk[94] given at the September 21, 2010 American Waterworks Association (AWWA) Water Security Congress. The metrics used to assess this progress were developed by the Critical Infrastructure Partnership Advisory Council (CIPAC) and were collected & aggregated by the Water Information Sharing and Analysis Center (WaterISAC). According to their study:

- More than 70 percent had incorporated security planning and design programs to all assets and facilities.
- More than 90 percent secure and monitor perimeters and have chemical safeguards in place.
- More than 80 percent control access to restricted areas by screening/inspecting people/vehicles who enter.
- More than 94 percent secure and monitor shipping, receipt and storage of hazardous chemicals.
- More than 85 percent integrated security and preparedness into budgeting, training and manpower responsibilities.
- More than 90 percent have developed emergency response plans.
- More than 50 percent are training, exercising, reviewing, and updating those plans.
- 75 percent are networking for collaborative responses in an incident.
- 86 percent have backup power for 24 hours; 50 percent for 96 hours (4 days) or more.
- 66 percent of water utilities can provide 91–100 percent of minimum daily demand for 24 hours.
- Almost 33 percent of water utilities can provide 91–100 percent of minimum daily demand for 72 hours.[95]

However, it is important to note that of the "22 Sector Specific Measures" which were used in this assessment, none of them addressed SCADA or Cyber security.

The good news is that there has been some progress in developing new resources to assist local water utilities to protect against cyber and other attacks. For example:

- Water ISAC. The Water Information Sharing and Analysis Center is "a highly secure Internet portal that provides the best source for sensitive security information and alerts to help America's drinking water and wastewater community

protect consumers and the environment." It is not a government program but was developed under a grant from the EPA by the Association of Metropolitan Water Agencies, as a resource to drinking water and wastewater utilities.[96]

- Training, information, and workshops on security issues are provided through the United States EPA, American Water Works Association, Water ISAC, and other affiliated organizations.
- Cyber Security Evaluation Tool (CSET), which is "a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems."[97]
- Threat Ensemble Vulnerability Assessment (TEVA)–program developed by the EPA, Sandia National Laboratories, and others to provide tools, software, and guidance to assist water utilities to implement real time monitoring for contaminants in the distribution system.

The American Water Works Association in 2004 estimated[98] that at least $1.6 billion is needed for public water systems to implement just the recommended first steps (fences, locks, etc.) in improving security, based on the vulnerability assessments. However, the federal government has not provided funding for this, and existing federal and state financial assistance to water utilities does not include funding for security improvements.

Securing the Control Systems

In March 2008, the Water Sector Coordinating Council Cyber Security Working Group published a *Roadmap to Secure Control Systems in the Water Sector* which "presents a vision and supporting framework of goals and milestones for reducing the risk of ICS [Industrial Control Systems] of the next ten years."[99] The *Roadmap* identifies the following as some of the "challenges" to reaching its goal to develop and deploy ICS security programs:

- Limited executive recognition of ICS security threats and liabilities.
- Lack of awareness about ICS security risks.
- Business case for ICS security has not been established throughout the water sector.
- Difficult or impossible to integrate new technologies into legacy systems.
- Implementation of security measures is often time consuming.

The "strategic framework" in the *Roadmap* seeks to achieve four main goals: 1) develop and deploy ICS security programs, 2) assess risk, 3) develop and implement risk mitigation measures, and 4) partnership and outreach. The *Roadmap* also describes 18 near-term (0-1 year) milestones, including "isolate ICS from public switch networks" and "Replace default security passcodes," but there are no "progress reports" available anywhere that detail how many of these milestones, if any, have been accomplished.

Serious Gaps Remain

While some progress has been made to better secure the U.S. drinking water infrastructure following 9/11, there are several serious gaps that need to be addressed. To begin with, the Bioterrorism Act does not provide clear lines of authority,[100] leading to some administrative overlap, duplication of effort, and confusion of roles between the EPA and Homeland Security. Neither the EPA nor Homeland Security has legal authority to order any water utility to take action to improve their security. Each water utility makes its own decision on whether to spend money if it has it to increase security.

Water utilities so far have only been required to complete a Vulnerability Assessment and an Emergency Plan—but have not been required to take any action to address the deficiencies revealed in their assessments. Further, these assessments do not adequately address terrorist threats but were designed to address more traditional and less costly threats such as vandalism and disgruntled employees. The EPA has not yet issued standards to the water utility community around which they can develop a baseline for water security.[101] And there is no requirement that these Vulnerability Assessments or Emergency Plans be updated or reviewed following their completion in 2003-2004. Most likely they are gathering dust on shelves all over the United States. Since the Vulnerability Assessments were exempted from state Freedom of Information Acts, no one outside the report writers and utility managers know what the vulnerabilities were or the status of any actions to address them. The information from Vulnerability Assessments has not been used to identify water security research needs or to allocate funds to water utilities to make needed security improvements.

These efforts also require funding, but not enough money has been made available to complete the Vulnerability Reports. While the maximum grant to a utility for completing an Assessment was capped at $115,000, the estimated cost for a very large utility to complete one was in the millions.[102] No federal funds have been made available to actually implement the recommendations of these Assessments, and there has been no overall assessment of how much this exercise may have made water utilities safer.

Finally, there is insufficient research on effects of chemical and biological weapons in drinking water, and how to best respond to such an attack on the water supply. Current practices for routine monitoring of water supplies for contaminants are inadequate for detecting chemical or biological contamination.[103] There has not been a strategic analysis on the national level of what it would actually take to achieve security—and what the metrics for that should be—for the national drinking water infrastructure.[104] These and other challenges must be mitigated in the years ahead if we are to avoid a major catastrophe involving the exploitations of the public water sector vulnerabilities identified in this discussion.

Conclusion

As summarized in Table 3, public water systems in the United States are vulnerable to attack by chemical and biological weapons and through their SCADA control systems.

While some progress has been made since the attacks on American on September 11, 2001, to strengthen the security of public water systems, serious gaps remain.

Table 3

Summary of Potential Locations and Types of Attacks

Potential Locations[105]

(1) At the source of water supply

(2) At the water treatment plant

(3) During storage of treated water (in the clear well, which is the reservoir in the plant which stores the finished water before being pumped to distribution)

(4) In the distribution system (mains, pipes, hydrants, blow-off valves, pump stations)

(5) In a buildings plumbing system, holding tanks, whole building water treatment system

(6) Through cyber attacks on the water systems SCADA control system network

(7) Through interdependencies (treatment chemicals, electrical power, etc.)

Potential Types of Attacks

(1) Chemical contamination

(2) Biological contamination

(3) Physical disruption

(4) SCADA disruptions

While public water systems nationally are facing a $220 billion shortfall over the next 20 years in the necessary funds to properly maintain and upgrade their physical assets, there is no funding program to provide to them the $1.6 billion (minimum) required to make essential security improvements to counter the known vulnerabilities. This funding should include the installation of real-time contaminant monitoring systems in water utilities nationwide, and the needed research on the impact of CBR agents in water and how to respond to a CBR contamination of a water supply.

Furthermore, as the *Roadmap* reveals, many water utility managers feel that the business case has not been made for the need to increase the security of their SCADA control systems. However, the development of Stuxnet and it's inevitable progeny, in addition to the inherent insecurity of water utility control systems, leave many water utilities wide open to cyber attack. Strong federal action is needed to put some teeth into the Roadmap process and to require water utilities to assess their vulnerabilities with their control systems and to address those deficiencies—with federal funding to help them get that done.

Action by Congress is needed to give the EPA the legal authority—and funding—to direct every water utility to take the action necessary to strengthen their physical and cyber security, to install real-time distribution system monitoring, and to implement the recommendations to remedy the vulnerabilities revealed in the vulnerability assessments and subsequent vulnerability reviews.

Finally, a strategic analysis on the national level needs to take place to define in concrete terms what it would actually take to achieve security in the drinking water infra-

structure, and the metrics for measuring the progress to that goal, with sufficient funding to accomplish it. Failure to do so could result in a major attack on our national drinking water through their cyber assets or the CBR equivalent of a 9/11 attack on the quality of our drinking water.

John McNabb is President of InfraSec Labs. He was an elected Water Commissioner in Cohasset, Mass. for 13 years, and has worked at the Massachusetts. Department of Environmental Protection and Clean Water Action. He has published several papers on water infrastructure issues and has presented papers at several technical conferences, including Black Hat and DEFCON.

Notes

1. This paper is an update and expansion of the subjects covered in the authors' DEF CON 18 presentation, *Cyberterrorism and the Security of the National Drinking Water Infrastructure,* http://www.defcon.org/images/defcon-18/dc-18-presentations/McNabb/DEFCON-18-McNabb-Cyberterrorism-Drinking-Water.pdf. The video of the talk can also be found on YouTube.
2. "*Water in the Universe*" by Vincent Kotwicki, Hydrological Sciences, Vol. 36, No. 1, February, 1991. He also points out that there are three theories of the origin of water on Earth (1) condensation of the early atmosphere, (2) outgassing from the interior of the primordial Earth, and (3) bombardment from comets and other extraterrestrial objects. Note that while the cometary bombardment theory has been very popular, it has been called into question by recent studies which show that the proportion of heavy water, called deuterium, found in cometary water are different than those found in the Earth's water. "*Earth's water probably didn't come from comets, Caltech researchers say"* http://neo.jpl.nasa.gov/news/news008.html
3. Wolf, Aaron T. (2001) "Water and Human Security," *Journal of Contemporary Water Research and Education:* Vol. 118: Iss. 1, Article 5. Available at: http://opensiuc.lib.siu.edu/jcwre/vol118/iss1/5
4. "*Water Scarcity & Climate Change: Growing Risks for Businesses & Investors*" A Ceres Report, The Pacific Institute, February, 2009.
5. "*Meeting the MDG drinking water and sanitation target: the urban and rural challenge of the decade.*" World Health Organization and UNICEF, 2006.
6. *Massachusetts Ground-Water Quality,* National Water Summary, 1986, pp. 297–304. http://wellowner2.org/SWQP/GWQ_Massachusetts.pdf
7. Critical infrastructure is defined in the Patriot Act (P.L. 107–56) as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*" (Sec. 1016(e)).
8. "*Money Down the Drain: How Private Control of Water Wastes Public Resources,*" Food & Water Watch, Washington, DC, February 2009.
9. "*Water: The Next Oil or an Infrastructure Play?*", Advisor Perspectives, 2008. http://www.advisorperspectives.com/pdfs/Water-The_Next_Oil_or_an_Infrastructure_Play.pdf
10. ITT *Value of Water Survey,* October, 2010. http://www.itt.com/valueofwater/media/ITT%20Value%20of%20Water%20Survey.pdf
11. See Water Conflict Chronology, Peter Gleick. http://www.worldwater.org/conflictchronology.pdf
12. See "*Water and terrorism*" by Peter Gleick, http://www.pacinst.org/reports/water_terrorism.pdf
13. For more on this attack, see the chapters by Bruce Hoffman, James Forest and Adam Dolnik in this volume.
14. See Jonathan Tucker, *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (MIT Press, 2000)
15. *al-Qaeda/al-Ablaj Threat Assessment v1.0 PUBLIC RELEASE VERSION 30 May 2003 02:00:01 EST / 07:00:01 GMT,* by Ben Venzke, IntelCenter, Alexandria, VA http://www.intelcenter.com/ATA-PUB-v1-0.pdf.

16. "*Food Defence Incidents 1950–2008: A Chronology and Analysis of Incidents Involving the Malicious Contamination of the Food Supply Chain*" by G. R. Dalziel, Centre of Excellence for National Security (CENS), S. Raratnam School of International Studies, Nanyang Technological University, Singapore, 2009
17. "*FBI: Biosecurity and the Select Agent Program*", presentation at the Select Agent Program Workshop, National Animal Disease Center, Ames, Iowa, May 10, 2011. http://www.selectagents.gov/resources/12.Will_So_FBI_SAP_workshop_Ames_5-10-2011.pdf
18. See Transcript of Presidents Bush's State of the Union address, at: http://www.washingtonpost.com/wp-srv/onpolitics/transcripts/sou012902.htm
19. A copy of this bulletin is available online at: http://www.mrws.org/Terror/Bulletin.html
20. *Chronology: the Plots.* http://www.pbs.org/wgbh/pages/frontline/shows/front/special/cron.html
21. See "From Baltimore Suburbs to a Secret CIA Prison," Washington Post (September 10, 2006), online at: http://www.washingtonpost.com/wp-dyn/content/article/2006/09/09/AR2006090901024.html
22. "*FBI: Al Qaeda Might Use Poison*" http://www.cbsnews.com/stories/2003/09/05/national/main571778.shtml
23. "FBI Hunts 4 Terror Suspects," CBS News (September 7, 2003), online at: http://www.cbsnews.com/stories/2003/09/07/national/main571952.shtml
24. *Osama Bin Laden Raid: Al Qaeda 'Playbook' Revealed,* ABC News, May 6, 2011. http://abcnews.go.com/Blotter/osama-bin-laden-raid-al-qaeda-playbook-revealed/story?id=13544154
25. "*Al-Qaeda suspect 'plotted to poison water*" http://mg.co.za/article/2011-08-20-alqaeda-suspect-plotted-to-poison-water/
26. *Challenges In The Water Industry: Fragmented Water Systems,* American Water, http://www.amwater.com/files/FragmentedWaterSystems012609.pdf
27. Wang, Jian-Weng and Li-Li Rong, *Cascade-based attack vulnerability on the US power grid, Safety Science*, Volume 47, Issue 10, December 2009, pp. 1332–1336.
28. "*Drinking Water Treatment Plant Design Incorporating Variability and Uncertainty*", Dominic L. Boccelli; Mitchell J. Small; and Urmila M. Diwekar, *Journal of Environmental Engineering*, 133:3, March 2007, pp. 303–312.
29. "*Drinking Water: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*" United States General Accounting Office, GAO-04-29, October, 2003.
30. "*A Secure and Resilient Water Sector*" presentation by Don Correll, President & CEO American Water, at US Chamber - Global Water Summit, March 18, 2010.
31. See *Chlorine: the Achilles Heel?* Presentation at the 2009 American Water Works Security Congress, by John McNabb. http://www.cohassetwater.org/pdf/chlorine_achilles_heel.pdf
32. *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options,* Updated September 12, 2008, Paul W. Parformak, Congressional Research Service, RL33206, page CRS-4. http://www.fas.org/sgp/crs/homesec/RL33206.pdf
33. *Proceedings of the First Annual Water Security Summit,* December 3-4, 2001, Hartford, CT, Haasted Press, see page 196 and then listen to the recorded session.
34. See *Analysis of the Massachusetts Drinking Water Infrastructure* by John McNabb, presented at the September 18, 2008 New England Water Works Conference, http://www.newwa.org/PDF/AnnConf08-SessC1040.pdf, and published in the December, 2010 *Journal of the New England Water Works Association*, http://www.southshorepcservices.com/Analysis_Mass_Water_Infrastructure-NEWWA-Dec2010.pdf
35. *Report Card on America's Infrastructure,* American Society of Civil engineers, http://www.infrastructurereportcard.org/fact-sheet/drinking-water. "*drinking water systems face an annual shortfall of at least $11 billion in funding needed to replace aging facilities that are near the end of their useful life and to comply with existing and future federal water regulation*s."
36. *Fatal Disease Outbreak from Contaminated Drinking Water in Walkerton, Canada,* Steve E. Hrudey, Association of Environmental Engineering & Science Professors Case Studies Compilations, 2006.
37. *The Legend of Camelford: Medical Consequences of a Water Pollution Accident,* Editorial by Anthony S. David and Simon C. Wessely, *Journal of Psychosomatic Research,* Vol. 39, No. 1, pp. 1–9, 1995.

38. *Boil order lifted, Woburn Advocate*, March 6, 2007. http://www.wickedlocal.com/woburn/local_news/x1108312282#axzz1XEuSJnj4
39. *Potential Contamination Due to Cross-connections and Backflow and Associated Health Risks,* US EPA, September 27, 2001.
40. *Water and Terrorism,* Peter Gleick, Water Policy 8 (2006) 481–503, http://www.pacinst.org/reports/water_terrorism.pdf
41. *Water and Terrorism,* pp. 494–495.
42. Please see the chapters in this volume by James Forest, Charles Ferguson and Joel Lubenau for more information about radiological materials.
43. GAO-04-29, *DRINKING WATER: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security,* October, 2003.
44. Kroll, Dan., "*Water distribution monitoring: opportunities and challenges for enhancing water quality and security.*" Hach Homeland Security Technologies White Paper July 2010, http://www.hachhst.com/wp-content/uploads/2010/07/White-Paper_-Enhancing-Security-in-Water-Distribution-System.pdf
45. Allman, pp. 2–3.
46. Allman, pp. 2–3.
47. Dennis C. Blair, Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," Statement for the Record, (February 2, 2010). Online at http://ww.dni.gov/testimonies/20100202_testimony.pdf
48. *Al Qaeda Training Manual*, Pavilion Press, 2006, pp. 120–124.
49. *An Al Qaeda Chemist and the Quest for Ricin,* by Joby Warrick, *The Washington Post*, May 5, 2004, page A01. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A2159-2004May4
50. *Recognizing waterborne disease and the health effects of water contamination: a review of the challenges facing the medical community in the United States,* Patricia L. Meinhardt, Journal of Water and Health, 04.Suppl, 2006, pp. 27–34.
51. Ibid.
52. See the website at http://www.WaterHealthConnection.org
53. *Recognizing Waterborne Disease and the Health Effects of Water Pollution: A Physician On-Line Reference Guide,* www.WaterHealthConnection.og
54. *Linking Public Health and Water Utilities to Improve Emergency Response,* R.J. Gelting and M.D. Miller, Journal of Contemporary Water Research and Education, Issue 129, October, 2004, pp. 22–26.
55. Online at http://www.epa.gov/watersecurity/pubs/water_security_handbook_rptb.pdf
56. Online at http://www.epa.gov/watersecurity/pubs/rptb_response_guidelines.pdf
57. Online at: http://www.epa.gov/safewater/watersecurity/pubs/small_medium_ERP_guidance040704.pdf
58. SCADA usually refers to highly distributed systems to control geographically dispersed facilities, and the term Distributed Control Systems (DCS) usually refers to the control systems in a localized facility such as a single treatment plant. However, we will use the term SCADA as a generic term to be inclusive of the larger systems as well as the localized systems, since for the purposes of this paper the same factors apply to a full-fledged SCADA as do to a DCS.
59. For a detailed description of the technological transition, see C4 Security, *The Dark Side of the Smart Grid–Smart Meters (in)Security,* (September 2009), online at: http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf
60. Many of them, however, still retain "always on" modem connections using phone lines, another potential route of attack by attackers who perform "wardialing" to find active modems and then exploit them.
61. "*Improving Security for SCADA Control Systems*" Mariana Hentea, *Interdisciplinary Journal of Information, Knowledge, and Management*, Volume 3, 2008, pp. 73–82.
62. GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems,* March 2004.

.org/?

JM: yes

63. "*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*", United States General Accounting Office, GAO-04-354, March 2004.
64. *Roadmap to Secure Control Systems in the Water Sector* (March 2008), p. 14. Available online at: http://www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf
65. Ibid.
66. The term "cyber event" is a broad term meant to encompass both unintentional and intentional compromise of a system from malware.
67. Online at: http://dataclonelabs.com/security_talkworkshop/papers/25550091-Proj-Grey-Goose-report-on-Critical-Infrastructure-Attacks-Actors-and-Emerging-Threats.pdf
68. *In the Crossfire Report,* Mcafee, January 28, 2010
69. *In the Dark - Crucial Industries Confront Cyberattack,* McAfee and CSIS, April 18, 2011.
70. *Common Cybersecurity Vulnerabilities in Industrial Control Systems,* Control Systems Security Program, National Cyber Security Division, Department of Homeland Security, May 2011.
71. Ibid.
72. It should be noted that this story is in dispute.
73. DHS only makes the last 10 reports available on their web site. I was able to obtain past reports from the repository maintained by Bob Johnston, CISSP http://dhs-daily-report.blogspot.com/, who has been downloading and storing the reports since 2004.
74. The incident reporting in these reports is not exhaustive, so one should not assume that these are all the incidents that actually occurred or that these numbers are representative of the actual incidence nationwide during 2010.
75. *Silver City Sun News*, March 11, 2010. DHS Open Source Report, March 12, 2010, p. 13.
76. *Lake Chelan Mirror*, June 23, 2010 http://lakechelanmirror.com/main.asp?SubSectionID=5&ArticleID=2670&SectionID=5
77. *Associated Press*, September 20, 2010. http://www.whotv.com/news/who-story-glidden-water-tower-092010,0,1010748.story
78. *New Canaan Patch*, December 4, 2010. http://newcanaan.patch.com/articles/computer-glitch-shuts-down-water-plant
79. Marc told the author that *". . . it was a rather straight forward pen test just compromising a series of systems using your standard Adobe and Microsoft related vulnerabilities. They suffered from the same problem as most places in that the actual control systems are not really ever patched, because of all the usual red-tape, which makes them easy to hack and really the only hard part was trying to find the private network (attached to the county network) where the control systems were located. That was the scary part about it like most of these pen test is that there was nothing james bond or interesting to it really. Sure plenty of the specific control software used in these environments has security flaws also but that does not matter when its an unpatched Windows 2000 system etc.*" Email from Marc Maiffret, April 18, 2011.
80. *Global Energy Cyberattacks: "Night Dragon"* white paper by McAfee Foundstone Professional Services and McAfee Labs, February 10, 2011.
81. A worm is a self-replicating program that, unlike a virus, does not have to infect a file to cause damage. Since many malicious programs these days utilize the features of worms and viruses, and also of trojans (which disguise themselves and non-malicious programs), the generic term "malware" is usually used.
82. *W.32 Stuxnet Dossier,* Version 1.4, February, 2011. Symantec Corporation.
83. Vulnerability Trends–SCADA Vulnerabilities, Symantec. http://www.symantec.com/business/threatreport/topic.jsp?id=vulnerability_trends&aid=scada_vulnerabilities
84. "*34 SCADA vulnerabilities revealed,*" Help Net Security, March 22, 2011. http://www.net-security.org/secworld.php?id=10771
85. For example, see: Statement for the Record of Sean P. McGurk Acting Director, National Cybersecurity and Communications Integration Center Office of Cybersecurity and Communications National Protection and Programs Directorate Department of Homeland Security Before the United States Senate Homeland Security and Governmental Affairs Committee, Washington, DC, November 17, 2010.
86. "*Son-of-Stuxnet"–Coming Soon to a SCADA or PLC System near you*". Eric Byres, May 31, 2011. http://www.tofinosecurity.com/blog/%E2%80%9Cson-stuxnet%E2%80%9D-coming-soon-scada-or-plc-system-near-you

87. Dennis C. Blair, Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," Statement for the Record, (February 2, 2010). Online at http://ww.dni.gov/testimonies/20100202_testimony.pdf
88. CIA -- Unclassified responses to the Questions for the Record from the Worldwide Threat Hearing on 6 February 2002, Senate Select Committee on Intelligence. http://www.fas.org/irp/congress/2002_hr/020602cia.html
89. *Cyberterrorism Hype v. Fact,* by Robert K. Knake, Council on Foreign Relations, February 16, 2010. http://www.cfr.org/terrorism-and-technology/cyberterrorism-hype-v-fact/p21434
90. *A view of cyberterrorism five years later,* Dorothy Denning, Center on Terrorism and Irregular Warfare, Naval Postgraduate School, Chapter 7 in *Internet Security: Hacking, Counterhacking and Society* (K. Himma ed.) Joes and Bartlett Publishers, 2007. In two emails to the author on June 30, 2010, Denning said that "*I also haven't seen anything to give me concern about the jihadists or change my overall assessment. . . . I would be very surprised if AQ has anything resembling a computer training center today. Maybe they did at one time, but it seems unlikely they would now. There are people who have associated themselves with AQ who have cyber skills, but I don't think any of them have the kind of skills needed to launch a serious cyber attack against a water system or any other critical infrastructure. Most of their skills relate to putting stuff on websites and protecting their cyber activities using tools like Tor and encryption. The jihadist cyber attacks are pretty rudimentary, e.g., web defacements and DoS attacks.*"
91. *Water Security Initiative Program Overview and Available Products,* EPA Fact Sheet,
92. Tiemann, Mary*, Safeguarding the Nation's Drinking Water: EPA and Congressional Actions,* September 30, 2010.
93. *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems,* Association of State Drinking Water Administrators National Rural Water Association May 30, 2002
94. *Measuring Water Security Progress,* L. Vance Taylor, AWWA Water Security Congress, September 21, 2010, National Harbor, Maryland.
95. Ibid.
96. WaterISAC Fact Sheet. http://www.epa.gov/safewater/watersecurity/pubs/waterISACFactSheet.pdf
97. Control Systems Security Program, US-CERT, http://www.uscert.gov/control_systems/satool.html
98. *Protecting Our Water: Drinking Water Security in America After 9/11.* American Water Works Association, 2004. http://fortressteam.com/resources/watersecurity.pdf
99. *Roadmap to Secure Control Systems in the Water Sector*
100. *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions,* Updated December 15, 2004, by Mary Tiemann, Congressional Research Service, RL31294. http://www.hsdl.org/?view&did=459643
101. *EPA needs a better strategy to measure changes in the security of the nation's infrastructure,* EPA Inspector General report, September 11, 2003. http://www.epa.gov/oig/reports/2003/HomelandSecurityReport2003M00016.pdf
102. "*Estimated costs for conducting a large system vulnerability assessment range from approximately $100,000 to several million dollars, depending on the complexity of the system. Additional resources are required to develop or revise the utility's emergency response plan. AWWA has estimated the total national cost to develop vulnerability assessments as required by the Bioterrorism Act to be approximately $500 million.*" Protecting our Water: Drinking Water Security in America After 9/11, American Water Works Association [no date]. http://fortressteam.com/resources/watersecurity.pdf
103. Nuzzo, Jennifer B. "The Biological Threat to U.S. Water Supplies: Toward a national water security policy," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science,* Volume 4, Number 2, pp. 147–159, 2006. Page 152.
104. Nuzzo, p. 157.
105. Ernest Lory, Stephen Cannon, Vincent Hock, Vicki VanBlaricum, and Sandra Cooper, "Potable water contamination and countermeasures," Naval Facilities Engineering Service Center, 2006. http://jocotas.natick.army.mil/ColPro_Papers/Hock.pdf