The Role of Technology in Enhancing Water Security: Protecting a Valuable Asset

Dan Kroll[a], Jeff Throckmorton[a]
[a]Hach Homeland Security Technologies, 5600 Lindbergh Drive, Loveland, CO USA 80539

ABSTRACT

Drinking water is one of the nation's key infrastructure assets that have been deemed vulnerable to deliberate terrorist attacks. While the threat to reservoir systems and water sources is deemed to be minimal, the vulnerability of the drinking water distribution systems to accidental or deliberate contamination due to a backflow event is becoming a well-recognized possibility. The myriad possible points of incursion into a distribution system and the ease of mounting a backflow event, combined with the fact that little or no quality monitoring occurs after the water has left the treatment plant, makes the danger of such an attack acute. This was clearly stated in a General Accounting Office (GAO) report to Congress that listed the vulnerability of the distribution system to attack as the largest security risk to water supplies.[1] Prior to this there has not been a system capable of detecting such an event and alerting the system's managers so that effects of an attack or accident can be contained. The general scientific consensus is that no practical, available, or cost-effective real-time technology exists to detect and mitigate intentional attacks or accidental incursions in drinking water distribution systems. The rapid detection and identification of breaches of security in the water distribution system is crucial in initiating appropriate corrective action. The ability of a technology system to detect incursion on a real time basis and give indications as to the cause could dramatically reduce the impact of any such scenario. As the vulnerability of the distribution system becomes more widely recognized, the development of a system such as the one described will be an invaluable tool in maintaining the integrity of the nations drinking water supply.

Keywords: Terrorism, Water Distribution, Monitoring, Sensor System

1. ARE OUR WATER SUPPLIES VULNERABLE?

The recognition that our water supplies are vulnerable to sabotage is not a recent discovery made after the attacks of 9/11. As early as 1941, after America had suffered another devastating surprise attack, FBI Director J. Edgar Hoover wrote, "Among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace. Obviously, it is essential that our water supplies be afforded the utmost protection." [2] The US Military also recognized the threat prior to 9/11. The historic department of defense policy that requires domestic military base reliance on local utility infrastructure whenever possible was explored and recognized as a threat by Major D. C. Hickman in his seminal report issued in September of 1999 entitled "*A Chemical and Biological Warfare Threat; USAF Water Systems at Risk.*"[3] There is a long history of water being vulnerable to such attacks.

- 1968 – Yippies threaten the Democratic National Convention in Chicago with plans to dump LSD into water supplies.[4]
- 1970 An informant revealed to the U.S. Customs Bureau plans by the radical Weathermen to steal biological weapons from Ft. Detrick, Maryland to contaminate a major water supply.[5,7,8]
- 1972 plot by ecoterrorist group R.I.S.E. to poison urban water supplies around Chicago. They were in possession of botulism, meningitis and anthrax as well as 40 kg of typhoid.[5,7,8]
- 1977 North Carolina reservoir sabotaged with poisonous chemicals.[6]
- 1979-1980 Two separate incidents of chemical poisoning cause 2008 illnesses in Virginia and Oregon.[5]
- 1980 Attempted extortion of a Lake Tahoe casino with threat to poison water.[5,7,8]
- 1980 Water mains in Pittsburgh deliberately contaminated with weed killer[5,7,8]
- 1983 After threats to poison water supply in Louisiana traces of cyanide found.[5,7,8]
- 1983 Israel uncovers Israeli Arab plot to poison Galilee water with "an unidentified powder".[5,7,8]
- 1985 Plutonium discovered in New York City's drinking water after a threat in an anonymous letter to contaminate the water supply. Not enough to cause a health threat.[5,7,8]
- 1987 In the Philippines, 19 police recruits died and about 140 are hospitalized after accepting water and sweets from unknown persons.[9]

Optics and Photonics in Global Homeland Security, edited by Theodore T. Saito,
Proceedings of SPIE Vol. 5781 (SPIE, Bellingham, WA, 2005)
0277-786X/05/$15 · doi: 10.1117/12.606940

- February 2002 Al Qaeda arrested with plans to attack U.S. embassy water in Rome with “cyanide”.[10]
- July 2002 Federal officials arrest two Al Qaeda terror suspects in Denver with documents in their possession about how to poison the country's water supplies[11]
- December 2002 Al Qaeda operatives arrested with plans to attack water networks surrounding the Eiffel Tower neighborhoods in Paris[12]
- April 2003 Jordan foils Iraqi plot to poison drinking water supplies from Zarqa feeding U.S. military bases along the Eastern desert.[13]
- September 2003 FBI bulletin warns of Al Qaeda plans found in Afghanistan to poison U.S. food and water supplies.[14]

That the water supplies are a target is also reinforced by the fact that domestic terrorist and fringe groups have shown continued interest in using a Chemical, Biological, or Radiological (CBR) agent in their attacks and Islamic terrorist groups have also exhibited interest in water supply systems as demonstrated by the more recent events detailed above. While these attempts were thwarted, as history shows, al Qaeda has a unique ability to diligently perfect and refine attack strategies. This threat is particularly important for U.S. military bases, as it is for private and government “icon” facilities. Researchers from the U.S. Air Force and Hach Homeland Security Technologies (HST) have calculated that an attack on drinking water distribution systems can be mounted for between $.50 and $5.00 per death, using rudimentary techniques, and amass casualties in the thousands over a period of hours.[15, 16] Mass casualties are a stated goal of Al Qaeda. Suleiman Abu Ghaith one of Osama bin Laden's closest friends and allies, said on an Islamic website said that the terrorists planned to attack the US with chemical or biological weapons. September 11 was "only a start. We have the right to kill 4 million Americans - 2 million of them children - and to exile twice as many and wound and cripple hundreds of thousands. It is our right to fight them with chemical and biological weapons, so as to afflict them with the fatal maladies that have afflicted the Muslims because of the Americans' chemical and biological weapons."[17] While the threat from Islamic terrorists is dire, it is not the only threat. Domestic terrorists and disgruntled employees may represent a scenario just as serious and possibly more likely.

2. HOW COULD AN ATTACK OCCUR?

When observing a typical municipal water supply system (Figure 1) it is natural to assume that the main point of vulnerability to a CBR attack would be the introduction of an agent into the system at the source water (reservoir) or treatment plant. However; in order to create widespread casualties from an attack on the source water, the amount of contaminant required would, after taking dilution into account, be either too large to handle easily or be more expensive than other readily available terrorist weapons. Within the water industry, this concept is summarized by the phrase *dilution is the solution to pollution.*

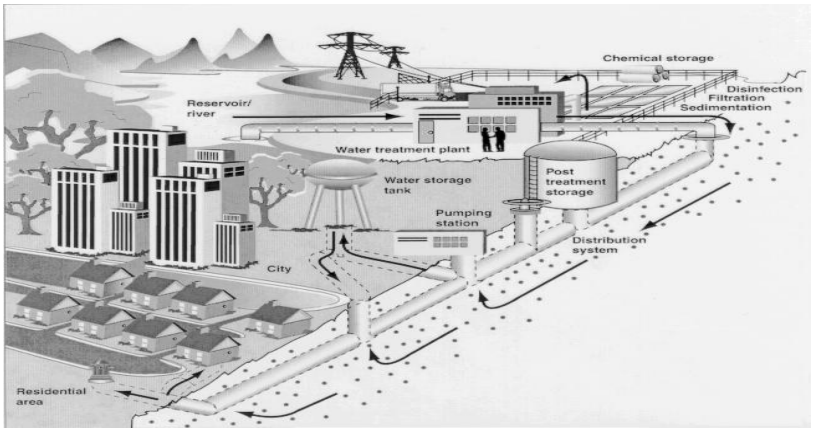

Figure 1 A representative municipal water supply system.

Initially after the attacks of 9/11, government experts declared that, due to this dilution factor, our water supply systems were fairly secure. Ronald Dick, FBI Deputy Assistant Director for Counter Terrorism Division, stated in testimony before congress that “In reality, targeting the water supply may prove difficult. In order to be successful, a terrorist

would have to have large amounts of agent."[18] EPA administrator Christie Whitman stated on 10/18/2001, "People are worried that a small amount of some chemical or biological agent – a few drops for instance – could result in significant threats to the health of large numbers of people. I want to assure people – that scenario can't happen. It would take large amounts to threaten the safety of a city water system. We believe it would be very difficult for anyone to introduce the quantities needed to contaminate an entire system."[19]

The concept of dilution providing security for the system was short lived. It wasn't long before government officials and industry experts realized that the crucial vulnerability to contamination was is the distribution system. By October 2003 a GAO report to the Senate stated that the distribution system was the area most vulnerable to attack.[1] Conceding that an attack with CBR agents would most likely take place somewhere in the distribution system, several misconceptions about this type of attack still persist. Historic (and incorrect) dogma holds that such attacks require the assistance of several technicians, are expensive to carry out, and require complicated and expensive pumping equipment to inject contaminants into a pressurized system. More recent studies by the Army Corps of Engineers, among others, show that CBR attacks could in fact be carried out for 50 cents or less per lethal dose, that a single individual can obtain or produce effective contaminants in quantity, and that contaminants can be introduced into the distribution system with the aid of inexpensive and easy to obtain pumping equipment via a method called *backflow attack*.[15,16,20,21]

3. WHAT IS A BACKFLOW ATTACK?

A backflow attack occurs when a pump is used to over come the pressure gradient that is present in the distribution system's pipes. This is usually around 80 lbs/in^2 and can be easily achieved by using pumps available for rent or purchase at most home improvement stores. After the pressure has been overcome and a contaminant introduced, Bernoulli effects pull the contaminant into the flowing system and the normal movement of water in the system acts to disseminate the contaminant throughout the network effecting areas surrounding the introduction point. The introduction point can be anywhere in the system such as a fire hydrant, commercial building or residence. See figure 2. Studies conducted by the US Air Force and Colorado State University have shown this to be a very effective means of contaminating a system.[22] A few gallons of highly toxic material was enough, if injected at a strategic location via continuous feed, to contaminate an entire system supplying a population of 150,000 people in a matter of a few hours. A terrorist could launch such an attack and be on a plane out of the country before the first casualties begin to show up.

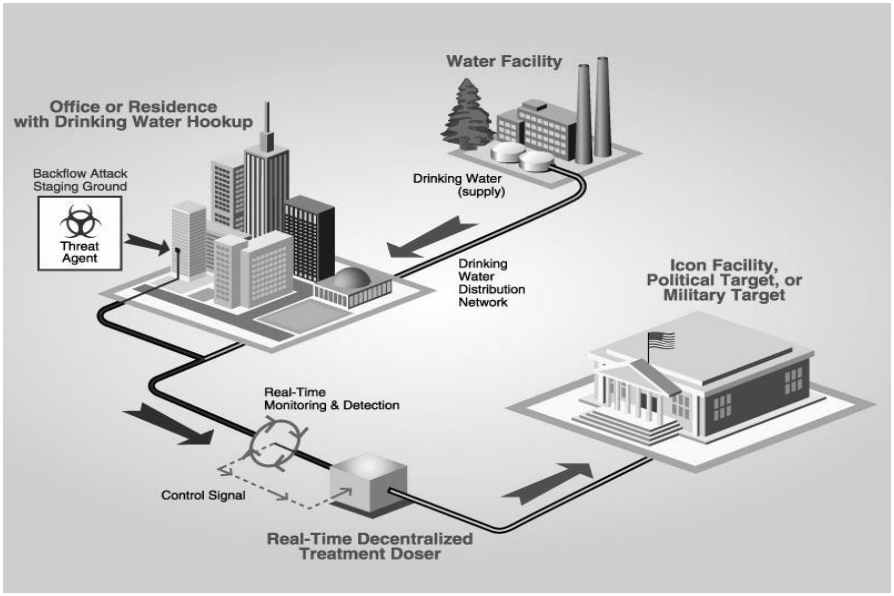

Figure 2. All distribution systems are vulnerable to backflow attacks.

Currently, monitoring of drinking water supplies in the distribution system is limited. Previous to the terrorist threat, it was not a priority. The ability to detect an event in the distribution system and then identify it would be of incomparable value in responding to an incident in a timely and proper manner. Such an ability would also serve the purpose of mapping a system for clean up, and after words, it could be used as a forensic tool to identify the source of an event. Prior to this, there has not been a device capable of detecting such an event and alerting the system's managers so that

the effects of an attack or accidental event can be contained. The general scientific consensus is that no practical, available, or cost-effective real-time technology exists to detect and mitigate intentional attacks or accidental incursions in drinking water distribution systems. The development of such a monitoring system was listed as by a panel of experts and industry leaders as a top priority in enhancing water security.[23]

3. WHAT SHOULD A MONITOIRING SYSTEM DETECT?

One of the problems when designing such a monitoring system for water is the vast number of chemical agents that could be utilized by a terrorist to compromise a water supply system tends to preclude monitoring on an individual chemical basis. Chemical warfare agents such as VX, Sarin, Soman, etc.; commercially available herbicides, pesticides and rodenticides; street drugs such as LSD and heroin; heavy metals; radionuclides; cyanide and a host of other industrial chemicals could be exploited as weapons. There are also a variety of biological agents and biotoxins that could be problematic. Which of the myriad possible agents would be the most likely to be deployed in a terrorist assault is sill a matter of conjecture. The possible number of chemical and biological substances that could be used in an attack is very large.[24] There are a variety of lists publicly available in the current literature, such as the list compiled by the CDC[25] and the military Tri-services list[26], specifying likely agents. There are also lists that have been compiled that are unavailable, due to security reasons, such as the list compiled by the EPA. Many of these lists are similar in composition, but no two lists are identical and in several cases are contradictory. To be truly effective a monitoring device needs to be able to detect any and all of the possible agents. A dedicated device capable of detecting anthrax for instance is interesting but not very practical, as it could be thwarted by the terrorist use of another agent. Also, another example is GC type systems that may be very effective for detecting volatile organics but would offer no protection against the introduction of a heavy metal agent such as mercury.

This need to detect such a wide variety of diverse contaminants requires a realignment of thinking from the traditional development of a sensor for a given compound or agent. Sensor arrays on a chip or the use of analytical instrumentation capable of detecting this variety is a definite challenge. Another approach is to use chemometrics to detect and characterize changes in basic water quality parameters and correlates them with threat agent introduction.

4. WATER ANAYSIS PRESENTS MANY CHALLENGES.

A common misconception concerning analysis in water is that the system is stable with little variation over time or from location to location. This is probably due to most analysts that are not specifically involved in water research being exposed to laboratory grade de-ionized water as the norm when running experiments. In the real world, even after treatment, there is great diversity in the water found in distribution systems. For a parameter as simple as pH that we would expect to be around 7 ± 1 pH units, the diversity is much greater and can run from 3 to near 11 pH units. Also in a given system there is great heterogeneity over time in basic conditions such as pH, turbidity, conductivity, etc. Figure 3 is representative of the diversity that can be found in the real world in these types of parameters over time.

On top of the great diversity of water quality that may be present in the distribution system, the general environment is also very harsh. The water conditions may be corrosive or scaling in nature. This can lead to degradation of anything placed in the system or the formation of a coating of various types of materials. See figure 4. There is also present in most pipe systems something known as biofilm. This is a thin layer of bacteria and their associated slime that coats the inside of pipes and any thing else present in the system. See figure 4. This layer of growth can coat sensors and render them unable to function properly. It can also clog small tubes and pipes used to draw off samples resulting in erroneous readings. Any detection system designed to function over long periods of time in the distribution system must be capable of handling these harsh conditions. There is also the problem of aging infrastructure. Many of the water pipes in our major cities are over 100 years old and are occluded with rust, crumbling concrete and other debris. Some of the pipes are actually still the original wooden pipes installed when the systems were first built. This raises concerns for instillation and sampling for a distribution system monitoring platform.

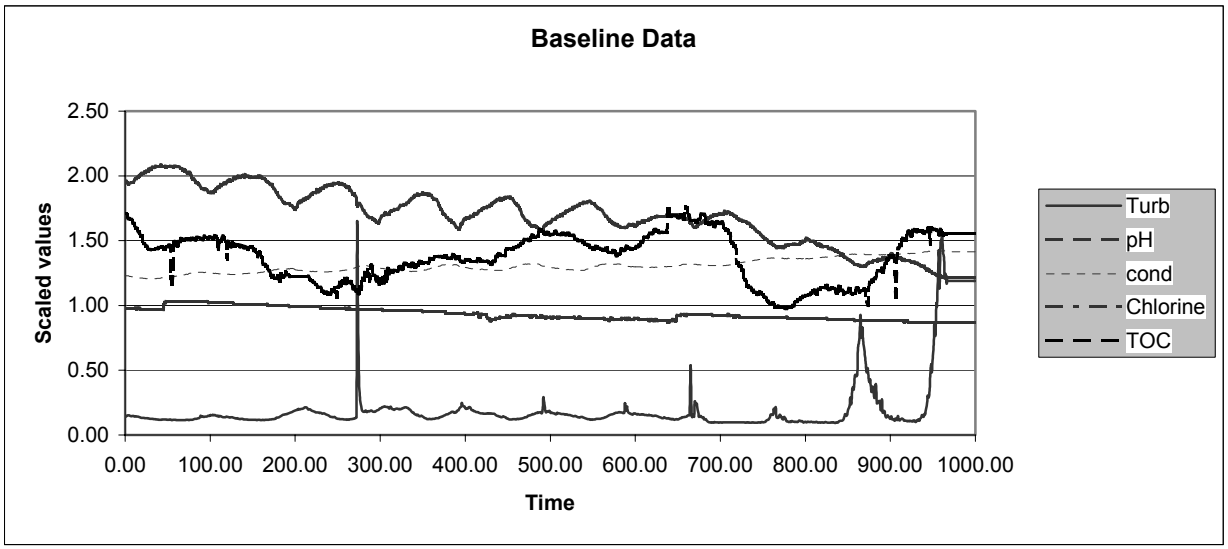

Fig. 3 Real world data can be complex and variable.

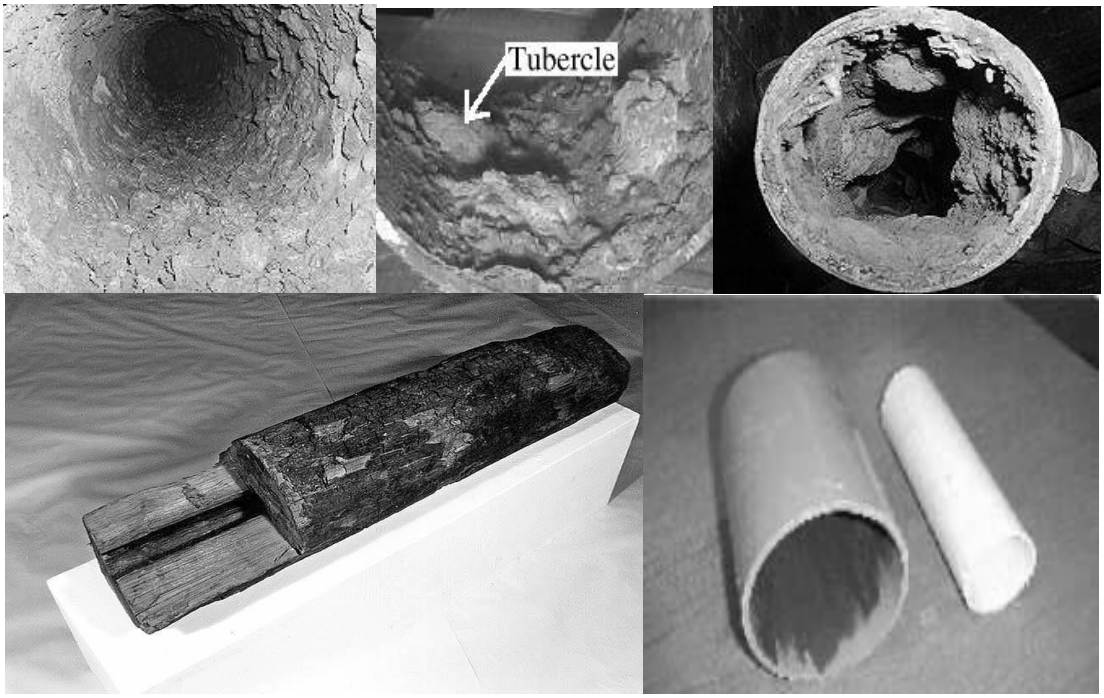

Figure 4. Photos show various forms of corrosion and scaling. The PVC pipe in the lower right hand corner is an example of biofilm. The lower left photo shows a wooden pipe.

5. COST CONSTRAINTS:

Do to the aging infrastructure plaguing most municipal water supply systems, drinking water and wastewater infrastructure investment costs over the next 20 years may range from $492 billion to $820 billion, according to a Congressional Budget Office (CBO) report.[27] This huge expenditure for needed upgrades leave little funding room for things such as security. This makes it very important that any sensor system be very cost effective. This goal of cost effectiveness can be addressed in two different manners. One is to design a very inexpensive system that could be

deployed for a low per customer cost. The other method is to develop a system that is capable of providing data that could be useful in decreasing the day-to-day operating costs of the system and improving general water quality.

A smoke detector can be used as an analogy. The relative low cost of smoke detectors allows their wide spread deployment to protect against an unlikely event. If smoke detectors were to cost several thousand dollars each few locations would be equipped with them. A water system protection device would be similar. Few municipalities would fund a system designed to solely protect against terrorist events, because of the low likelihood of their occurrence in a given location, unless it were very inexpensive. The market could and would bear a higher cost for a dual use device that could help streamline general operations and help to provide increased water quality, hence providing real value even if a terrorist event never occurs.

6. THEORIES OF DEPLOYMENT AND OPERATION.

It is extremely unlikely that in the near future an effective system will be developed at such a low cost point that every household will be able to be outfitted with a monitoring platform. As instrumentation become available for monitoring in the distribution system they will most likely not be inexpensive. Due to this, the day when we are able to protect every house hold is not liable to be soon. A network approach utilizing instruments with different capabilities and cost points will need to be employed to provide the most coverage and protection possible for the funds available. See Figure 5. While not every point will receive complete protection a network approach has the best chance of detecting an event early in its onset and alerting the operators of the system so that they can make the crucial decisions that will be needed to limit the damage being done. If an attack is detected early consumers can be warned not to use the water. Also though the turning off of valves it may be possible to isolate the contaminant plume to a small area before the entire system becomes unusable.

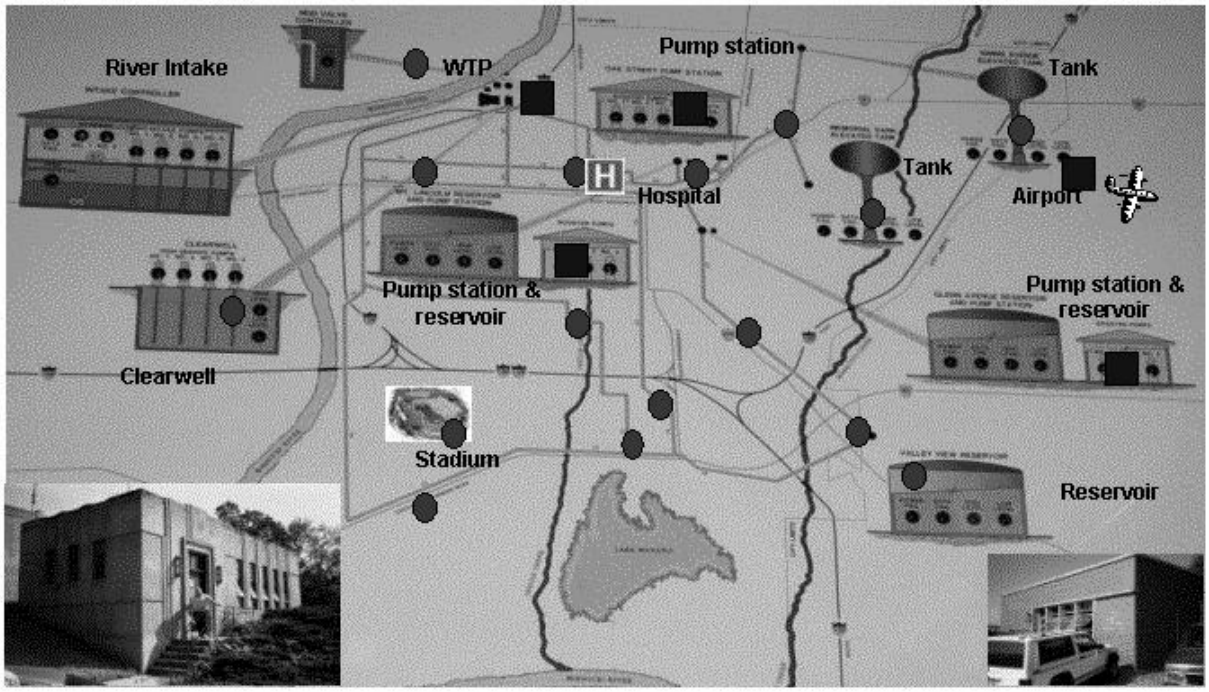

Figure5. Network deployment strategy. Squares represent possible deployment sites for a more expensive platform combined with circles that are possible deployment sites for a mid priced solution used in conjunction with the higher priced systems.

The ability to contain and isolate an incident is critical in limiting the number of casualties. It is also imperative to limit clean up of any incident. The anthrax clean up for the Hart Office building after the contaminated mail incident cost the EPA over $27 million from its super fund site.[28] Clean up procedures for the different agents will vary. The Army Corp of Engineers in conjunction with Hach HST is currently conducting research into the fate and transport of various threat

agent types in the distribution system. Important questions such as the degree of absorption to different pipe materials still remain to be answered. Once these factors are determined more in-depth research into clean up methods can be conducted. It is possible that some agents will not be able to be cleaned up and piping will need to be replaced. This could be a very expensive proposition when it is considered that not only main pipes may need to be replaced but some household plumbing as well. Also, if the agent is widely disseminated in buildings due to aerosolization many structures may need to be abandoned. Therefore, the need to contain is critical in reducing casualties and in limiting clean up costs.

This need to rapidly warn and contain brings up the topic of communication systems. If an analytically competent sensor system is developed, there still needs to be means of communication to link the sensors to the operators and the operators to field workers and the public. There are many options for the communication systems from hard lines to wireless. Any communication system should be designed to be secure so as not to be prone to hacking that could disable the system or instigate false alarms.

7. ON-LINE TREATMENT

The need to respond quickly to an incident to limit damage leads to the concept of on-line treatment. See figure 2 and figure 6. Once you have the ability to detect an incursion into the system the next step would be to link the detection system to a treatment platform. Due to the wide variety of threat agents that could be found, simple chlorination boosters are probably not adequate. In fact simple chlorination may increase the toxicity of some compounds. A more effective means of treatment will probably include a combination of chemical addition with various other methods of treatment. Methods that are being investigated include UV, pulsed UV, pulsed power, electron beam, pulsed ion and others. If the detection system was capable of making a classification the treatment could be tailored to the specific threat to deliver treatment type and doses adequate to deal with the problem. While not all of the contaminated water would be likely to encounter the treatment point, lessening of the amount of contaminant present in the system could save lives and mitigate property loss.

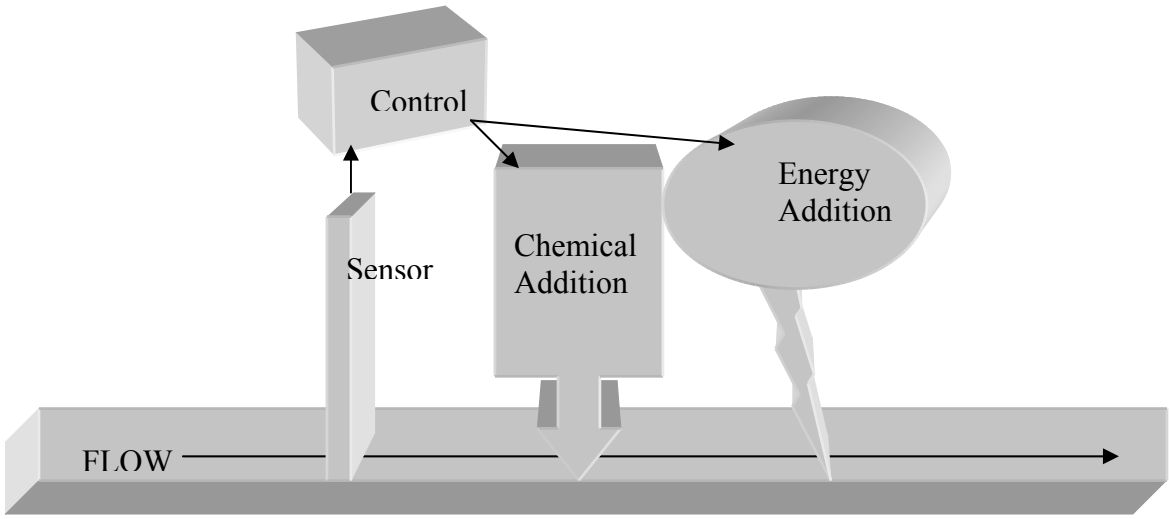

Figure. 6. Diagram of an on-line on-demand treatment system.

8. CONCLUSION

The threat to the nation's water supply is a real risk that could result in a huge loss of life, impairment of the public psyche, and property damage to the extent that the economy could be affected. Historic actions of terrorist groups and continuing interest in this form of attack points to the recognition of the susceptibility that our water distribution system have to such an event. Due to the dilution factor in source water, the majority of the vulnerability is in the

distribution system. There is a dire need for an analytical solution to the problem of monitoring for such incursions. There are a wide diversity of technologies currently being investigated for use in these monitoring scenarios. As research into these areas continues it is important to keep certain key aspects of the problem in mind. Chief among these is the need to understand the conditions present in the distribution system, the wide variety of threat agents that could be introduced and the monetary constraints placed on deployment of such a system. As research continues methods will be forthcoming that will not only help to detect and contain such attack if they occur, but that will hopefully also lead to a greater understanding of the conditions present in the system on a real-time basis and hence will result in an overall increase in water quality supplied to the end user even if terrorist activity never occurs.

REFERENCES

1) *GAO-04-29* "Drinking Water Security: Experts' views on how future federal funding can best be spent to improve security"; October 2003

2) Hoover, J.E. Water Supply Facilities and National Defense. 1941. *Jour. Awwa,* 33:11:1861

3) Hickman, Maj. Donald C, USAF, BSC, "A Chemical and Biological Warfare Threat: USAF Water Systems at risk," Counter Proliferation Paper No. 3, USAF Counter Proliferation Center, Air War College, September 1999.

4) Linder, D.O., "The Chicago Seven Conspiracy Trial" http://www.law.umkc.edu/faculty/projects/ftrials/Chicago7/Account.html

5) Terrorism Research Group, Rand Corporation (No Date), "Chronology of chemical-biological incidents"

6) Clark, Richard Charles, 1980. *Technological Terrorism*. Old Greenwich, CT: Devin-Adair.

7) Falkenrath, R.A., R.D. Newman and B.A. Thayer (1998) "*America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*." MIT Press, Cambridge, MA.

8) Ownbey, P.J., F.D. Schaumburg, and P.C. Klingeman (1988) "Ensuring the security of public water supplies" *Journal of the American Water Works Association* 80(2) 30-34.

9) Purver, R. (1995) "Chemical and Biological Terrorism: The Threat According to the Open literature" Canadian Security Intelligence Service.

10) BBC News. "Cyanide attack foiled in Italy" Wednesday, 20 February 2002, http://news.bbc.co.uk/1/hi/world/europe/1831511.stm

11) Cameron, Carl. Fox News, "Feds Arrest Al Qaeda Suspects with Plans to Poison Water" Tuesday, 30 July 2002. http://www.frwa.net/ARTICLES/feds_arrest_al_qaeda_suspects_wi.htm

12) Von Derschau, V. Associated Press "Radicals Arrested Near Paris Over Poison Gas Attack Plot" 18 December 2002

13) Feuer, A. *New York Times*. "Jordan Arrests Iraqis in Plot to Poison Water" Wednesday, 2 April 2003.

14) CBS News "Al Qaeda Might Use Poison" 5 September 2003. http://www.cbsnews.com/stories/2003/09/05/national/main571778.shtml

15) Kroll, Dan, confidential paper, "Mass Casualties on a Budget", 2003, Hach HST

16) Army Corps of Engineers Calculations on threat agents and requirements and logistics for mounting a successful backflow attack.

17) Lines, A. *Daily Mirror*. "Al Qaeda: We'll Kill 4 Million More Americans" 14 June 2002. http://66.218.71.225/search/cache?p=Suleiman+Abu+Ghaith+4+million+americans&toggle=1&ei=UTF-8&u=www.mirror.co.uk/news/allnews/page.cfm%3Fobjectid%3D11950702%26method%3Dfull%26siteid%3D50143&w=suleiman+abu+ghaith+million+americans&d=9EF65E0A40&icp=1&.intl=us

18) Dick, R.L. Statement for the Record of Ronald L. Dick, Deputy Assistant Director, Counter Terrorism Division, and Director, National Infrastructure Protection Center, Federal Bureau of investigation Before the House Committee on Transportation and Infrastructure Subcommittee on Water Resources and Environment October 10, 2001.

19) Whitman, Christie, EPA Press Release Thursday, Oct 18, 2001. Environmental News Whitman Allays Fears for Water Security; Possibility of Successful Contamination is Small.

20) ASHRAE Satellite Broadcast: Homeland Security for Buildings; 14 April 2004.

21) Waterborne CBR Agent Building Protection; V. F. Hock, S. Cooper, V. Van Blaricum, J. Kleinschmidt, M. D. Ginsberg, E. Lory; Proceedings of the National Association of Corrosion Engineers Exposition, 2003.

22) Allman, T.P. "Drinking Water Distribution System Modeling for Predicting the Impact and Detection of Intentional Contamination. Masters Thesis. Summer 2003. Dept. of Civil Engineering. Colorado State University. Fort Collins, Colorado.

23) Office of Science and Technology Policy, The White House, "The National Strategy for the Physical Protection of Critical Infrastructures and Assets," February 2003.

24) Kroll, Dan. "Utilization of a New Toxicity testing system as a Drinking Water Surveillance Tool" *Water Quality in the Distribution System.* Edited by William C. Lauer. AWWA Press 2004.

25) CDC Emergency Preparedness and response website. http://www.bt.cdc.gov/agent/agentlistchem.asp and http://www.bt.cdc.gov/agent/agentlist.asp

26) US Army Center for Health Promotion and Preventive Medicine. Short-term Chemical Exposure Guidelines for deployed Military Personnel. May 1999.

27) Water Infrastructure Network News. http://www.win-water.org/win_news/112702article.html

28) Ramstack, T. Washington Post. "GAO Scores Contractor Work, Pay in Hart Anthrax Clean-up. 18 June 2003.