Secure Water Supply

M. D. Ginsberg, V. F. Hock
U. S. Army Engineer Research and Development Center
P.O. Box 9005, Champaign, IL 61826-9005

A.G. Pappas
Edgewood Chemical & Biological Center
Aberdeen Proving Ground, MD 21010

ABSTRACT

Previous to 9-11, it was assumed that a combination of small-scale bench testing plus dimensional analysis would be sufficient to model fate and transport of chemical and biological (CB) contaminants in water systems. Water security is a life safety issue. Water supply systems on military installations and forward facilities are vulnerable to both conventional, industrial and military CB agent contamination by terrorists. The pre 9-11 generation of sensors could not directly detect many common CB agents, and the few sensors that could were very expensive. The pre 9-11 generation of water distribution simulations cannot correctly model CB agent uptake on the pipe walls of a distribution system. Therefore the outcome of an attack via CB agents in the water supply is not well understood.

In the post 9-11 environment, the EPA, ECBC, and ERDC stakeholders concluded that the pre-existing fate and transport models should be updated to include results from meso-scale testing. The Water Security Research Test Loop (WSRTL) is designed to help update these models with meso-scale testing of fate and transport of CB agents. The WSRTL would also serve as a test-bed to facilitate new generations of sensor technology and water treatment technology.

This research is responsive to several DOD initiatives including:

1. CINC's and services are required by DoDD 2000.12 and DoDI 2000.16 standard 26, to conduct a higher headquarters vulnerability assessment of their installations AT programs every three years.
2. The updated dynamic simulation tools can be used to support the Joint AntiTerrorism Guide (JAT Guide)
3. The Joint Future Operational Capability (JFOC) for fixed facility collective protection.

1. DESCRIPTION OF A TYPICAL WATER DISTRIBUTION SYSTEM.

Figure 1 provides an excellent overview of a generic water distribution system. Fresh water is pulled from a reservoir, treated, and stored in a series of holding tanks and associated pumping stations. Water is then distributed via a network of underground pipes. It is important to note that potable water and water for fire suppression are distributed through the same pipe network. This generic system design has several inherent weaknesses: the distribution network has no redundancy; the service area subtends a large geographical area; and there is a lack of anti-tampering devices. [GAO 2003]

2. COMMON MISCONCEPTIONS ABOUT ATTACKS ON WATER DISTRIBUTION SYSTEMS

On initial inspection of the water distribution layout represented in Figure 1, it is tempting to guess that a chemical or biological agent could be introduced at the water reservoir or the treatment plant. This method of attack would allow the attacker to act at some distance from the kill zone. The attack may have one of two basic objectives: denial of service or human casualties. As the system has few redundant components, a denial of service attack at the reservoir or treatment center is a real possibility, especially through the use of high explosives. In order to create widespread casualties, however, the amount of contaminant required to permeate the whole system would, after taking dilution into account, either be too large to handle expeditiously or far more expensive than other readily available terrorist weapons. Within the water distribution industry, this concept is summarized by the phrase *dilution is the solution*. Hence, a CB attack capable of causing casualties must be initiated close to the target facility.

Conceding that an attack with CB agents must take place somewhere in the distribution system close to the target, several misconceptions about this type of attack still persist. Current dogma holds that such attacks require the assistance of several technicians, are expensive to carry out, and require pumping equipment to inject contaminants into a pressurized system. [ASHRAE 2004] More recent studies by the Corps of Engineers, among

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 DEC 2004	**N/A**	**-**

4. TITLE AND SUBTITLE **Secure Water Supply**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U. S. Army Engineer Research and Development Center P.O. Box 9005, Champaign, IL 61826-9005; Edgewood Chemical & Biological Center Aberdeen Proving Ground, MD 21010**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**6**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

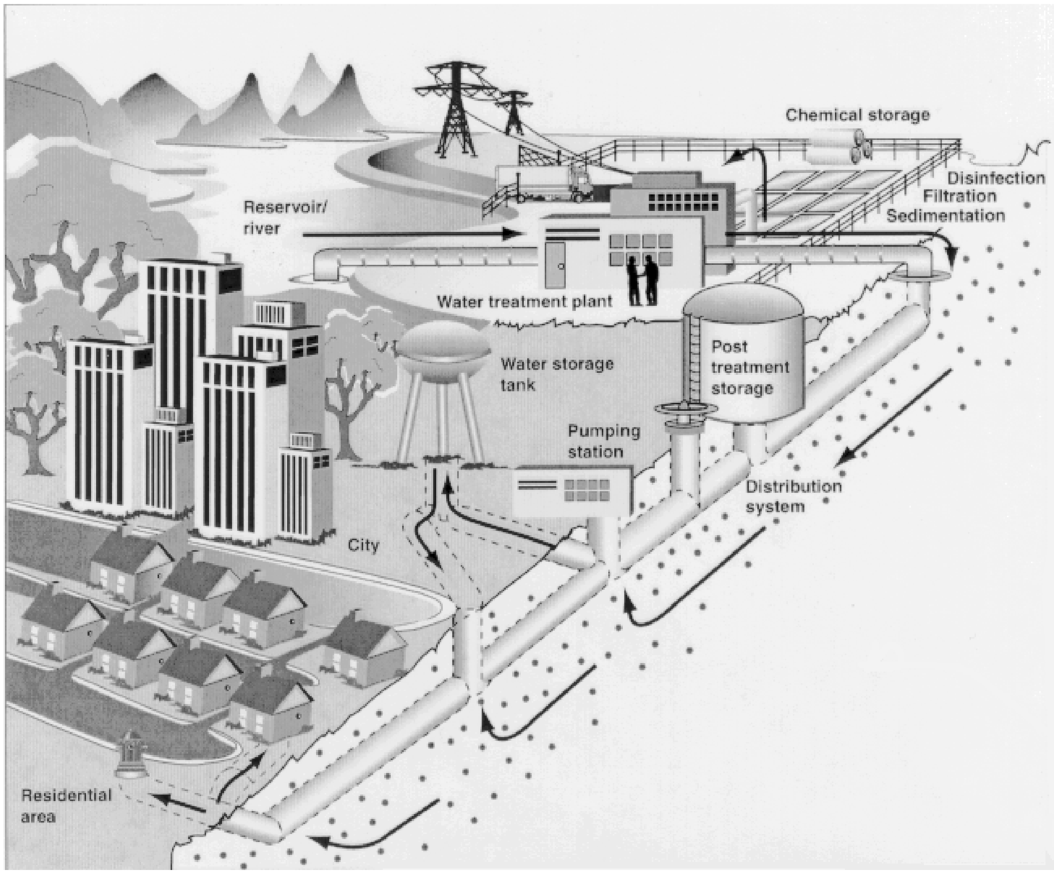

Figure 1. Representative municipal water distribution system.

others, show that CB attacks could in fact be carried out for as little as 80 cents 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 without the aid of pumping equipment via a method called *backflow attack*.

The single most common misconception of how to handle a contaminated water distribution system is to "just shut the water off." Such a response would have several undesirable effects. Stopping the water flow within the system does not halt the spread of the contaminant via diffusion. Additionally, many components in water distribution systems are severely stressed under loss of pressure and can easily fail, so pipe implosion and various forms of valve and pump failure are likely. Also, a system shutdown does not simply mean that customers need to find another source for consumption; it means that important industrial operations and fire protection services will be interrupted for the duration.

3. TREATMENT AND CLEANUP

The speed and assurance demonstrated during treatment and cleanup after an attack are crucial to restoring user confidence in the water distribution system. Even a series of minor delays or missteps in the recovery of this key utility could lead to years of consumer mistrust.

The two most likely forms of attack on a water distribution system are electro-mechanical damage (e.g., from an explosion) and contamination (e.g., CB agents).

Electrical and mechanical damage are repaired with comparative ease because such damage, albeit in less severe forms, is commonly encountered in everyday operations. Damage from construction equipment or weather events, for example, are sufficiently common that maintenance personnel are experienced or familiar with cleanup and repair procedures.

By comparison, attacks using CB contaminants are virtually unseen by most system operators, and countermeasures may vary depending on the particular agent used. Indeed, given the large array of readily available CB agents, a comprehensive list of contaminants and their corresponding treatment and cleanup methods would be difficult to collect. For example, there are many decontamination methods for pipe systems, including flushing, scouring, swabbing or pigging, jetting or balling, chemical cleaning, and cleaning and re-lining. These methods have coverage rates that range from 60 m to 5 km of pipe per day. The cost of these methods is inversely proportional to the coverage rate. [Ellison et. al.]

In order to address a terrorist attack that uses contaminants, there is a long list of science and engineering questions to which responders need reliable answers. Examples include the following: What zones are affected? How rapidly will the affected zones change? Can a temporary treatment device be inserted at a key point in the system? What method should be used to decontaminate the system? Given the large number of potential contaminants, the variety of treatment methods available, and the rarity of such events up to the present time, some form of computerized decision support tool could prove useful. The foundation for any such tool would be a complete understanding of the physicochemical aspects of CB agent fate and transport within a water distribution system. Section 6 summarizes our current knowledge on the topic.

4. IS SUCH AN ATTACK LIKELY?

Having stated that a terrorist attack on a water distribution system can be inexpensive, carried out with methods that are not technically difficult, and requires technical finesse in the response, one must estimate if such an attack is likely given the current strategic methods used by terrorists.

Terrorist attacks are part theater. [Hoffman 1971] A terrorist attack is intended to have meaning both to the victim's peer group (i.e., the terrorized) and to observers who are actually or potentially sympathetic with the terrorists' cause. The result must be easily communicated to and understood by both groups. Hence, most attacks are chosen because they are easily interpreted in video and still pictures. A crashed airliner, a burning building, or explosions do not require explanation in multiple languages to be understood by an international audience. For example, the current insurgency in Iraq has been careful to make detailed video recordings of their terrorist acts. These video recordings then appear on DVDs that are used as recruiting tools.

In this context, an isolated terrorist attack on a water distribution system seems unlikely. Pictures of water-damaged buildings caused by a broken water main have little ability to terrorize. The result of a CB agent attack could only be explained by pictures of sick or dead victims, and interviews with witnesses and relatives. These make poor video footage, and are dubious as recruiting tools. This line of reasoning does not mean that an attack on a water distribution system is unlikely; it means the form of such an attack is more likely in two particular scenarios.

In one scenario, the attack on a water supply is not carried out in isolation, but is one phase of a compound attack. A dual attack could start with a denial of service attack on a water supply followed by arson or bombings in the affected service area. The initial denial of service attack can either take the form of destroying a water main or inducing authorities to shut down a system due to contamination concerns. The complementary attack would be designed to cause maximal fire damage while the fire suppression water supply is unavailable.

A second scenario is to forgo the attack's value as a video publicity opportunity and target a fixed facility with the intention of disrupting the target nation's ability to respond to terrorist acts. Examples of such targets would be fixed military facilities engaged in mobilization or logistic support, fixed military facilities engaged in command and control of a deployed force, or selected government facilities engaged in law enforcement or judicial proceedings. Additionally, fixed facility targets might also include foreign facilities strongly associated with U. S. interests, including embassies, commercial buildings, or manufacturing facilities.

5. RESEARCH GOALS FOR THE WRSTL

Before 9-11 it was assumed that a combination of micro-scale bench testing in combination with dimensional analysis would be sufficient to model the fate and transport of CB contaminants in water systems. That is, it was assumed that bench-scale testing could yield results that were valid for distribution systems of all sizes through the application of scaling laws. Although it was known that specific scientific facts about larger systems could not be resolved by a combination of bench testing and scaling laws, the additional expense of building a test bed at a larger scale did not seem prudent before 9-11.

The U.S. Army Engineer Research and Development Center (ERDC), Environmental Protection Agency (EPA), and Edgewood Chemical Biological Center (ECBC) have cooperatively designed and constructed the Water Security Test Loop facility located at Edgewood Arsenal, MD. This meso-scale test loop supports testing of actual CB agents (i.e., not simulants) in pipe loops of varying length. This test bed has features that simulate various methods of introducing contaminants to the loop, a flexible layout that can incorporate new sensors and treatment equipment as necessary, a SCADA system capable of automatic supervision of experiments and implementation of automated control systems, and replaceable pipe sections where aged field samples of pipe with varying properties can be inserted and tested [Hock et al 2003]. In this way the test loop can also be used to test a cleanup strategy before implementation in response to an actual attack.

5.1 Technological Innovations

The WSRTL is currently being used to facilitate rapid development in several key technology areas. The key results are listed by technology area.

5.1.a. Sensors

New generations of sensors have been enabled using the combined resources of ERDC, ECBC and the WSRTL. The new sensor technology can be grouped into two broad classes.

a.) Agent specific sensors – With various research partners, a new generation of sensors has been developed that can detect CB agents with excellent specificity and sensitivity. Based on micro-optical techniques, these sensors take advantage of the ready availability of adsorbers based on single-stranded DNA.

b.) Generalized sensors – recent results have shown that standard water parameters (ex. temperature, pH, conductivity, oxidation-reduction potential, etc.) can be combined to discriminate the chemical or biological class of CB agent present.

5.1.b. Models

The following is a short list of current engineering models that describe fate and transport of contaminants. These models have been in use for more than a century, and are likely to have some shortcomings (which are also listed).

Wall Interaction: Both wall interaction and turbulence use the classical relation $\frac{u}{v*} = f\left(\frac{yv*}{\eta}, \frac{y}{e}, \frac{y}{L}\right)$ where u is water velocity, y is the distance from the wall, e is the roughness height, L is the pipe diameter, η is the viscosity, and v* is "friction velocity" i.e., $= \sqrt{\rho / \tau_0}$ where ρ is the density and τ_0 is the shear stress the fluid exerts on the pipe. This calculation assumes that CB agents cannot adhere to or be absorbed by pipe walls, which is incorrect. Pipe walls consist of a wide range of materials, some of which accumulate only after the pipe has been in use. These include water deposits (e.g., tubricles), corrosion products, and biofilm. Figure 2 shows examples of pipes with such deposits. It is quite likely that contaminants interact with pipe wall material. If so, extra terms would need to be represented in the expression derived above. The exact terms would depend on the nature of the contaminant-wall interaction, such as diffusion, chemical reaction, adhesion, etc. An extreme example would be a biological agent settling permanently in the pipe's biofilm.

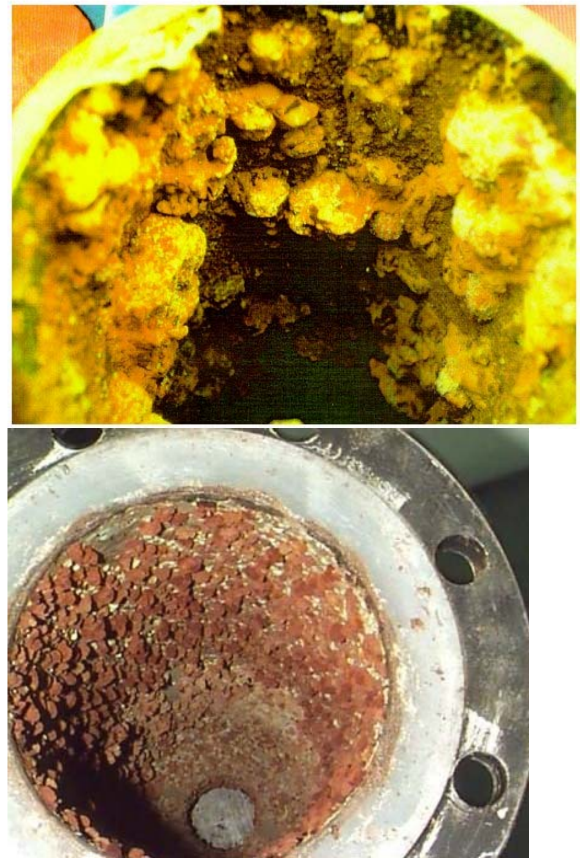

Figure 2. Examples of water distribution internal pipe deposits.

Reaction Rates: In modeling fate and transport of contaminants, it would be helpful to know the reaction rates between water treatment chemicals and the contaminant. The classical relation between two reactants is rate = $k[A]^m[B]^n$ where [A] and [B] are the molar concentration of the two reactants, m and n are unknown constant exponents, and $k = \exp(-E_a/rT)$ with E_a being the Arrhenius constant, r being the universal gas constant, and T being temperature. Unfortunately, this expression does not hold at low concentrations in the presence of corrosion products, chlorine, biofilm, scale, or decontamination products. Additionally, intermediate products of contaminant breakdown can be more toxic than the original contaminant, thus requiring mathematical modeling of several different reactions simultaneously.

Updating these classical results enables development of control systems to monitor sensors, engage countermeasures, and predict the duration of an attack.

5.1.c. Water Treatment Technology

Some water treatment chemicals that are suitable for CB agent destruction are in themselves hazardous and cannot be used in a potable water distribution system. The meso-scale test-bed has enabled the study of non-hazardous "green" alternative disinfectant treatments such as ozone, UV, Pulsed Corona Discharge and other advanced oxidizing and non-oxidizing technologies for both installations and forward facility applications.

A database summarizing treatment and cleanup methods (see section 4) with a list of the contaminants most likely to be used, could assist in hastening the response time to an attack. In addition, computer software also could be interfaced with new sensor and water treatment technology. New-generation sensor technology can now measure the concentration and distinguish among dozens of classes of contaminants. Also, transportable water treatment devices (that can be placed just downstream of an attack site) are now available, as are *green* systems that do not produce toxic breakdown products.

6. FUTURE RESEARCH.

As the engineering models of fate and transport are refined, computer-based simulations of a CB attack will also have better fidelity. With improved models and simulations, new engineering applications become feasible including:

1. *Pre-planning response strategies* — personnel can be trained or try out various techniques in advance.
2. *Vulnerability assessments* — simulating different attack scenarios on existing infrastructure can accomplish several goals, including formulating recommendations for changes to existing infrastructure, modifying or refining planned additions to existing infrastructure, etc.
3. *Placement of new resources* — this includes optimal placement of sensors, pre-positioning of treatment equipment, etc.
4. *Design of automated response systems* — when used to protect critical fixed facilities and using a combination of new sensor and treatment technologies, it seems reasonable to plan for control systems capable of monitoring the sensors and automatically engaging treatment technology when necessary.

To support these applications, research is currently underway or planned to fill the various knowledge gaps discussed earlier, such as interaction between contaminants and pipe wall constituents, reaction rates in a potable water environment, sensitivity and specificity of new sensor technologies, and efficacy of *green* water treatment technologies.

7. CONCLUSIONS

7.1 Army Impact:

Current Army plans to modernize the force include shifting the physical position of the command and control infrastructure away from the theater and to home-based fixed facility (i.e. the "flagship" concept). This reduces the "footprint" of fielded troops and minimizes the required logistics capacity into the theater of battle. Having fixed facilities as an integral part of the force increases the need to provide effective and proportional response to CB attack on the fixed facilities' water distribution system. ex. A strategy of "shut down the system and evacuate the building" is not tactically feasible if it denies an effective command and control structure to troops in the field. Having an effective and proportional response relies on three key enabling technologies: sensors, decontamination strategies, and control systems.

7.2 Summary.

Water distribution systems are vulnerable to two broad forms of attack: denial of service and contamination. Denial of service can be accomplished on a wide scale using either physically destructive methods or contaminants that force operators to shut down the system. Physically destructive methods can be used successfully at any scale, but an attack by contaminants must occur relatively close to the selected target if the intended result is to produce human casualties. Contrary to conventional wisdom, contaminant attacks do not require sophisticated technicians, pumping equipment, or huge investments.

Because conventional distribution systems are not redundant, they are vulnerable to dual attack. In such an attack, the most important mistake to avoid is a reactive shutdown of the system without regard to fire suppression.

Speedy and effective response to an attack is vital to restoring public confidence in the system.

Several federal agencies have cooperated in the construction of a meso-scale water security test loop to fill in current engineering knowledge regarding CB attack, and to assess new sensor and treatment technologies.

REFERENCES

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

Ellison, D., Duranceau, S.J, Ancel, S., McCoy, R.; Investigation of Pipe Cleaning Methods; Awwa Research Foundation; Denver CO.

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

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

Hoffman, A.H.; 1971; Steal this book (A Handbook of survival and Warfare for the Citizens of Woodstock Nation: This Book will end free speech); Pirate Editions, N.Y.

Patalon, W.; 2004 May 15, Security: The Army's Edgewood center develops systems to detect tainted water and cleanse contaminated buildings. Baltimore Sun.