Office of Homeland Security & Preparedness
Intelligence Bureau

The Potential Terrorist Risk of Drinking Water Contamination

Key Findings

- Both domestic and international terrorist groups have expressed interest in contaminating drinking water in the United States, and domestic groups have attempted to do so with some success. However, there are no known threats to New Jersey's Water Sector at this time.
- The types of contaminants most likely to be used by terrorists are biological and chemical agents that are accessible, not easily susceptible to degradation, and that overcome the dilution, filtration, and disinfection aspects of the drinking water process.
- The Storage and Distribution stage of the drinking water process is the stage most vulnerable to contamination. More specifically, although it has yet to become a conventional threat, backflow contamination – increased pressure on the user side of the connection, forcing water and contaminants back into distribution pipelines – debunks traditional thought regarding the feasibility of drinking water contamination, in that it requires fewer resources and can be instigated at access points such as fire hydrants and most types of residential and commercial connections.

Risk Overview

Domestic terrorist groups have historically threatened, and in some cases have executed contamination of drinking water systems. Such groups are likely to continue targeting the Water Sector in the future. These groups include, but are not limited to, hate groups, eco-terrorists, anti-government and religiously motivated groups. International terrorist groups, specifically Islamic extremists such as al Qaeda, have shown interest in contaminating US drinking water. However, contaminating drinking water is not known to be a characteristic attack of these groups, and it is not as sensational as an attack using explosives. The State of New Jersey Terrorism Threat Assessment, May 2008 concludes that homegrown terrorists* are more likely to attack in the near future than international groups such as al Qaeda – although an al Qaeda attack would probably be more catastrophic. Homegrown terrorists may find drinking water contamination more appealing, as they have fewer resources and would be less capable of organizing and carrying out a sensational, large-scale al Qaeda-type attack. Additionally, "lone-wolf" actors may be capable of

* Homegrown militant Islamic extremists are self-generating US-based extremist entities (individuals or groups), which are inspired and guided by militant Islamic extremist ideology but do not receive direct orders from foreign actors such as al Qaeda.

such an attack, and some have been found to possess significant amounts of contaminants in the past.

Contaminating drinking water could endanger public health via direct contamination, and adversely affect overlapping sectors such as agriculture, health, fire suppression, and power generation. The psychological effects of contamination of the drinking water supply would be far-reaching and long-lasting. This could result in public panic and create a loss of confidence in the ability of government and industry leaders to protect consumers.

Previous instances of terrorists obtaining contaminants, as well as some successful introductions of contaminants into water systems, demonstrate the feasibility of successfully targeting drinking water. Table 1, at the end of this assessment, outlines specific threats to the water sector in the United States based on open-source reporting. The data includes 26 incidents which date back to 1968. These incidents were selected based on the perceived credibility of the threat, and to demonstrate the variety of groups and methods associated with water contamination.

Types of Contaminants

The Environmental Protection Agency (EPA) has identified over 200 contaminants of interest for intentional drinking water contamination, based on health and dispersal effects.[1] To be most effective, these contaminants would need to withstand the dilution, filtration, and disinfection effects of the water process. This could be achieved by using contaminants in high quantity, of high potency, or those that are not easily susceptible to degradation. Terrorists would most likely seek out contaminants that are available and accessible on the open market.

Chemical contaminants may be readily accessible, as many industrial chemicals can be obtained online, while other chemicals such as insecticides are available at hardware and feed stores. Additionally, chemical contaminants may be more resistant to chlorine treatment than many biological pathogens, making them an attractive option for terrorists.[2]

Biological pathogens are often more difficult to obtain and store, and effective delivery would be complex and require specialized knowledge. While biological agents tend to be less accessible than their chemical counterparts, they are still appealing as potential contaminants to the water supply, as can be seen in historical incidents in Table 1. Additionally, as technological development continues, cultivating biological contaminants will become easier, thereby making pathogens more appealing for use in water contamination.

Methods and Points of Access for Contamination

Raw Water Sources

Many threats received regarding the contamination of drinking water discuss introducing the contaminant into the drinking water supply by adding a toxin to a raw water source, such as a

reservoir. Intakes[†] are the part of the raw water stage that has the most potential for intentional contamination. Raw source water is often easily accessible, and targeting the source stage of the process would allow the attacker to act farther from the kill zone. However, due to the size and residence time of water in the raw source stage, a very large amount of contaminant would be necessary to create significant contamination of drinking water. Furthermore, because this is the pre-treatment stage of the process, contaminants that are not easily susceptible to degradation and that are able to maintain their toxicity throughout the treatment processes would be required for effective contamination.

Treatment

Contamination at the treatment stage of the process could be executed via physical tampering with filtration equipment or via cyber attacks. Physical tampering with filtration equipment alone could allow unsafe water to pass to the distribution system, but it would be most effective when accompanied by introducing contaminants.

Tampering at the treatment stage could also be accomplished via cyber attacks on the Supervisory Control and Data Acquisition (SCADA) system, the computer network that monitors and controls the drinking water process. Using cyber methods to contaminate drinking water could cause chemical underdosing/overdosing, disabled service, reduced pressure flow, overflow of untreated sewage into public waterways, or the sending of false information to operators to prevent awareness of real-time operating conditions. A recent example of a cyber intrusion into utilities overseas is informative. According to a recent statement by Tom Donahue, a senior CIA analyst, "We have information, from multiple regions outside the United States, of cyber intrusions into [electric] utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."[3] Additionally, Table 1 includes incidents of cyber intrusions which date back to at least 1994. (For additional information, please refer to the OHSP product**:** The Cyber-Terror Threat, available on the OHSP secure Web site at www.state.nj.us).

Storage and Distribution

Instances of vandals gaining access to finished water storage tanks are also cause for concern, as they demonstrate the feasibility of access to this stage of the drinking water process. In most cases, water in storage tanks will not be treated again before reaching the consumer; the amount of water in storage tanks is considerably less than sources in the supply stage, and would require less contaminant for a successful attack.

[†] An intake is a place or opening at which a fluid is taken into a channel, pipe, etc. In this instance, it is the point at which source water is taken into the water system and to the treatment stage.

According to a 2004 Government Accountability Office report, as well as industry experts, the distribution system is the stage most vulnerable to intentional contamination.[4] Distribution is a post-treatment stage of the drinking water process that includes bottling companies and distribution pipelines. Contaminated drinking water can also affect bottling and food processing companies, which often draw their water from the local supply. This could allow contaminated water to reach a broader public.

A potential method of contamination in the distribution stage is backflow contamination. Backflow contamination involves changing the pressure in the distribution pipes to alter the flow and push used/non-potable water or other substances from any domestic, industrial, or institutional piping system back into the drinking water distribution system. Backflow can be initiated inexpensively and without specialized knowledge or access to water supply network facilities. This method of contamination would allow easier access, since the introduction point could be any residential or commercial facility or fire hydrant within the distribution network. It also requires contaminants of less potency, as this occurs in a post-treatment stage of the process.

Consequences

The economic losses of an attack on the Water Sector would be considerable, as documented in the 1993 unintentional contamination of water with *Cryptosporidium*[‡] in Milwaukee. The damage to infrastructure, as well as cost to the health-care sector and government agencies involved in this case, totaled around $96 million. The financial consequences of contamination vary. For example, oil-based contaminants would be more difficult to remove from the drinking water system and may require costly replacement of equipment that could be time-consuming, thus increasing the duration of a denial of service and increasing the cost of replacement of infrastructure. Furthermore, the food and beverage industry, which largely uses water from a local system in the production of its products, would be adversely affected by water contamination.

Outlook

An August 2008 posting on a Web site linked to al Qaeda demonstrates a continued interest in drinking water contamination against the West. The post calls for an attack on the drinking water of major cities and includes tips on how to carry out such attacks, specifically citing the use of distribution pipelines to do so.[5] Authorities have also found documents in the possession of individuals in the United States linked to al Qaeda, regarding how to poison water supplies. According to an interview with a senior al Qaeda member in May 2003, "The al Qaeda organization said that it will use new methods of fighting the Americans, indicating its intention to poison the drinking water of several American states."[6]

[‡] Cryptosporidium is a parasite that is resistant to chlorine disinfection. It is one of the most frequent causes of waterborne disease among humans in the United States.

While contamination at the supply stage is a common terrorist threat to the Water Sector, the amount of contaminant required for a successful attack makes it a less likely threat. The treatment stage of the process is less accessible and would require a physical or cyber breach on the facility. Traditional thought regarding the feasibility of drinking water contamination is that an attacker would need large amounts of an agent, significant knowledge of the water supply network, and access to critical locations in the system. However, our assessment is that this may not be the case, as demonstrated in the vulnerability of the storage and distribution stage. While it has yet to become a conventional threat, backflow contamination would provide an effective way of contaminating drinking water post-treatment with fewer resources. With backflow, access is not an issue, because it can be initiated at any service connection or hydrant.

Potential Indicators of Pre-Operational Planning

Pre-operational planning indicators that could lead to intentional water contamination include:

- Surveillance and reconnaissance;
- Probing to identify reactions of security units to threat indicators;
- Photographing/video-recording sites;
- Excessive note-taking/audio recording;
- Trespassing;
- Vandalism;
- Signs of tampering with security equipment, such as cameras;
- Theft of a marked utility vehicle, identification badges, or uniforms;
- Compromised/breached security measures – for example, locks, fences, hatches;
- Unauthorized access of sites, facilities, or computer systems;
- Threats to the sector or specific facilities.

At this time, we have no specific intelligence indicating that an attack on the US or New Jersey water supply is imminent. However, international and domestic terrorist groups have demonstrated their intent and capability to contaminate drinking water. This threat warrants ongoing situational awareness within the law enforcement community and private sector.

Suspicious activity involving the water sector should be treated as having a possible nexus to terrorism, and be reported immediately to the New Jersey Office of Homeland Security and Preparedness (OHSP) at 866-4-SAFE-NJ and to local law enforcement authorities.

Figure 1

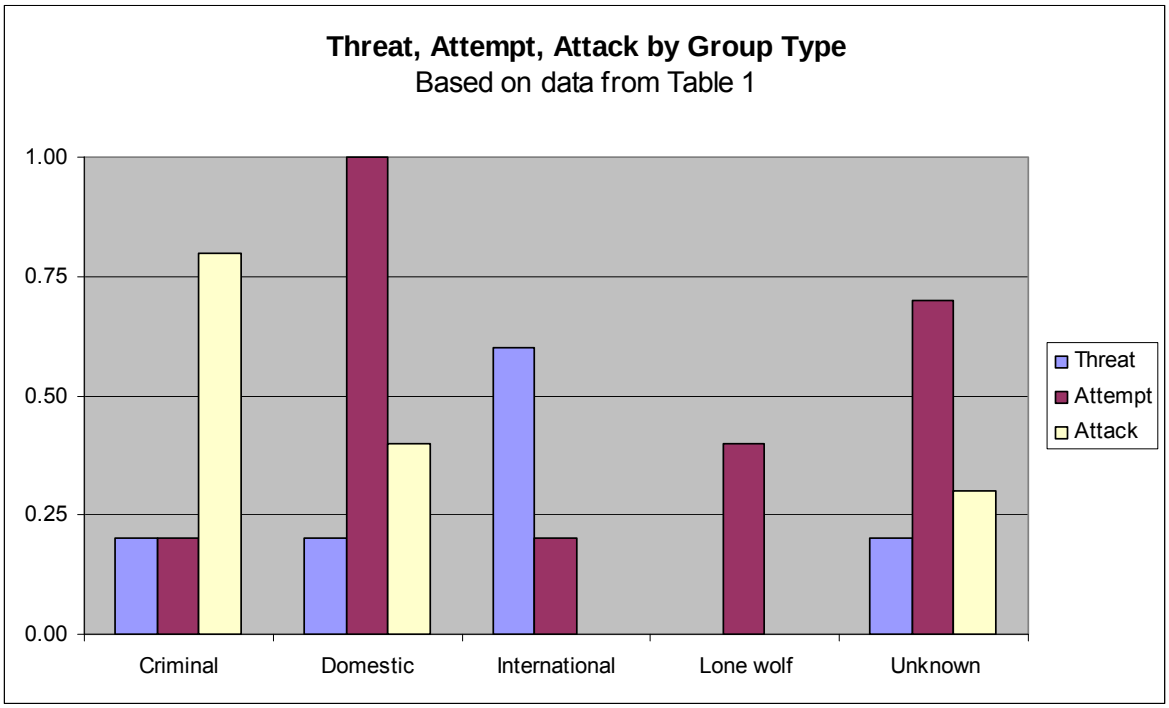
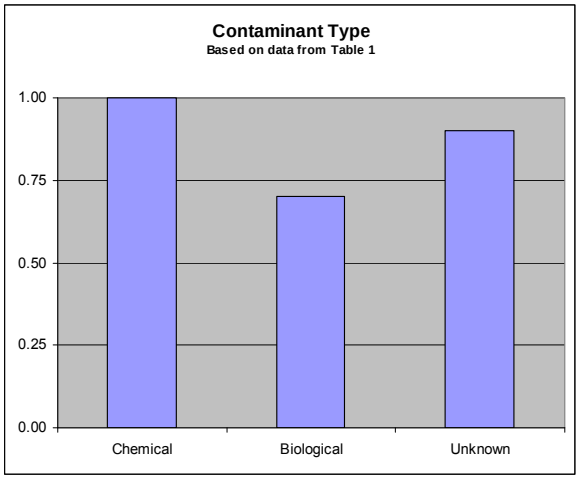


Figure 1[§] demonstrates the intent and capability of various types of actors to contaminate drinking water, based on data from Table 1. This data supports the analysis that international groups would be less likely than domestic or homegrown groups to select water contamination as a method of attack. It also illustrates that while lone-wolf scenarios are less common, these actors may be capable of such an attack, as demonstrated by individuals from Table 1 who were found to possess a significant amount of contaminants.

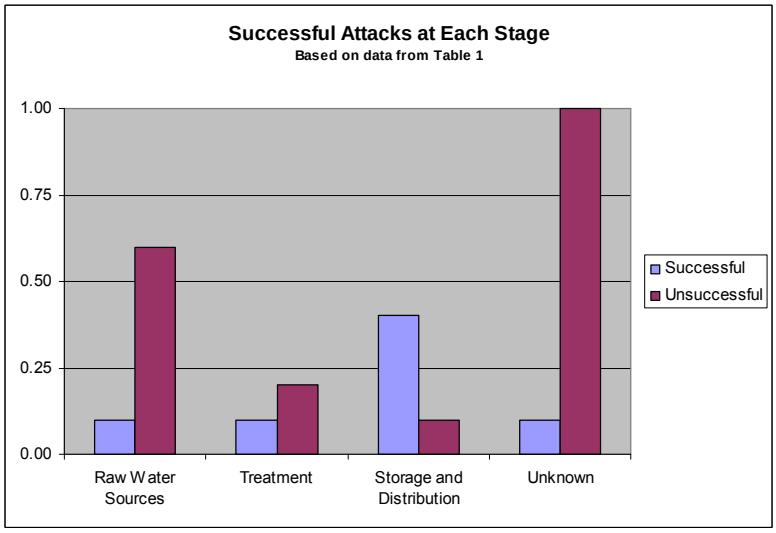
[§] Incidents are graphed in each Figure relative to each other by setting the largest value equal to 1. Every other value is divided by the original largest value and graphed accordingly, allowing for relative comparison among incidents. For example, in Figure 1, lone-wolf attempts occurred at 40 percent of the frequency of domestic attempts.

Figure 2



Biological pathogens are often more difficult to obtain and store, and effective delivery would be complex and require specialized knowledge. While biological agents tend to be less accessible than their chemical counterparts, they are still appealing as potential contaminants to the water supply, as can be seen in Figure 2, which depicts types of contaminants used in the Table 1 threats.

Figure 3



According to a 2004 Government Accountability Office report, as well as industry experts, the distribution system is the stage most vulnerable to intentional contamination.[7] This analysis is supported by Figure 3, which illustrates successful attacks at each stage of the drinking water process, based on the data in Table 1.

Table 1:
Specific Open-Source Threats of Water Contamination in the United States

Date	Location	Incident	Known Efforts or Access to Contaminants	Stage Threatened or Infiltrated	Party Responsible	Party Type
1968	US	Threat to dump LSD into water supply	No	Source	Weathermen	Left-Wing
1970	Fort Detrick, Maryland	Attempt to acquire biological contaminants for water supply from Fort Detrick, Maryland	Yes	Source	Weathermen	Left-Wing
1972	New York	Threat to contaminate Kensico Reservoir with nerve gas	No	Source	*Unknown*	*Unknown*
1972	Chicago; St. Louis	Arrests in Chicago of individuals with 30-40 kg typhoid cultures to poison water. Unlikely to cause serious problems due to chlorination.	Yes	Source	Order of the Rising Sun	Hate group
1972	Chicago	Group possessed botulism, meningitis, anthrax, typhoid.	Yes	Source	R.I.S.E.	Eco-terrorist
1977	North Carolina	Contamination of reservoir with poisonous chemicals and removal of safety caps/valves	Yes	Source	*Unknown*	*Unknown*
1980	Lake Tahoe, Nevada	Attempted extortion of casino with threat to poison water	No	*Unknown*	Individual	Criminal
1980	Pittsburgh	Water mains deliberately contaminated with weed killer	Yes	Distribution	Individual	Criminal
1982	Los Angeles	LAPD arrested man preparing to poison city's water with biological agents.	Yes	*Unknown*	Individual	Lone wolf
1983	Louisiana	Threats to poison water supply. Traces of cyanide found.	Yes	*Unknown*	*Unknown*	*Unknown*
1984	Dalles, Oregon	Salmonella in glasses of water to two commissioners	Yes	Distribution	Rajneeshee cult	Religious
1984	Dalles, Oregon	Contaminated water tank for city with Salmonella. 750+ cases outbreak.	Yes	Distribution	Rajneeshee cult	Religious
1984	New York, Chicago, Washington, DC	Drum of potassium cyanide to use to poison water systems. The group believed God would ensure no Aryans would be killed. Unlikely to cause serious problems due to insufficient amount of contaminant.	Yes	*Unknown*	The Covenant, the Sword, and The Arm of The Lord	Hate group
1985	New York	Plutonium in drinking water after threat in anonymous letter. Not enough to cause a health threat.	Yes	*Unknown*	*Unknown*	Criminal
1994	Phoenix	Hacked into SCADA system. The particular system monitored water level only.	Yes	Cyber	Individual	*Unknown*
1998	East St. Louis, Illinois	50-gallon drum of cyanide to poison water of major cities	Yes	*Unknown*	The New Order	Hate group
2002	Rome, Italy (US Embassy)	Cache of potassium ferrocyanide. Targeted US Embassy.	Yes	*Unknown*	Salafist Group for Call and Combat	Islamist
2002	Denver	Al Qaeda suspects in US with documents about how to poison water supplies	No	*Unknown*	Ujaama brothers	Islamist
2002	Salem, Massachusetts	Arrest man who has 5 pounds of mercury for threat to dump in a local lake, which provides drinking water	Yes	Source	Individual	Lone wolf
2003	Greenville, South Carolina	Package with ricin in container and note threatening to poison water supplies if demands unmet	Yes	*Unknown*	*Unknown*	Criminal
2003	US	FBI bulletin warns of al Qaeda plans found in Afghanistan to poison US food and water supplies.	No	*Unknown*	Al Qaeda	Islamist
2004	US	FBI and DHS bulletin warning terrorists were trying to recruit workers at water utilities to poison drinking water	Yes	*Unknown*	*Unknown*	*Unknown*
2006	Harrisburg, Pennsylvania	Plants virus and spyware in water treatment system. Could control chlorine output.	Yes	Cyber	*Unknown*	*Unknown*
2007	Willows, California	Sabotage water canal by installing unauthorized software and damaged computer that diverts water from Sacramento River	Yes	Cyber	Individual	Criminal
2007	Letcher County, Kentucky	Sand stones dumped into water tank	Yes	Distribution	Individual	Criminal
2008	N/A	Posting on a Web site calling for attack on drinking water of Western cities	No	Distribution	Al Qaeda	Islamist

Successful Act of Contamination

Endnotes

[1] Environmental Protection Agency's On-Scene Coordinators/Criminal Investigations Division Training for Water Sector Emergency Response, May 2008.

[2] Pitchforth, Nikolai, "Threat of Water Supply Bioterrorism: Who Will It Impact?", *Water & Wastes Digest*, Volume 41, Number 12, December 2001, <http://www.wwdmag.com/Threat-of-Water-Supply-Bioterrorism-Who-Will-It-Impact--article2816>

[3] SANS Institute, "CIA Confirms Cyber Attack Caused Multi-City Power Outage," SANS NewsBites, Volume X, Issue 5, January 18, 2008, <http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5>

[4] Government Accountability Office, GAO-04-1098T, "Drinking Water: Experts' Views on How Federal Funding Can Best Be Spent To Improve Security," September 30, 2004, <http://www.gao.gov/htext/d041098t.html>

[5] MEMRI, "Islamist Forum Member Proposes Poisoning Water Systems of Major European Cities," August 2008.

[6] Venzke, Ben, *al-Qaeda/al-Ablaj Threat Assessment*, (Alexandria, VA, IntelCenter, 2003), p. 6.

[7] Government Accountability Office, GAO-04-1098T, "Drinking Water: Experts' Views on How Federal Funding Can Best Be Spent To Improve Security," September 30, 2004, <http://www.gao.gov/htext/d041098t.html>

We welcome your comments concerning this document.
Please complete the attached survey so that we can continue to serve your needs.

For further information on this document or other OHSP analytical products, please contact the OHSP Intelligence Bureau at OHSPINTEL@ohsp.state.nj.us or 609-584-4000, ext. 7.