Figure 1: The planned Hoover Dam bypass project was expedited after 9/11 to improve safety and security. *(Ubergirl [own work], CC BY-SA 3.0, http://creativecommons.org/licenses/by-sa/3.0)*

Hydroterrorism: A Threat to Water Resources

Robert B. Sowby

Abstract

Hydroterrorism—a form of terrorism in which water is the tool or the target—is intensifying, especially in water-scarce regions. Recent incidents in the Middle East and past incidents elsewhere illustrate that water resource systems are vulnerable to both physical and virtual attacks with impacts to water infrastructure, public health, and the environment. This paper introduces the problem, presents pertinent examples, and offers some direction for response to an often-overlooked national security issue.

Introduction

Lake Mead and Hoover Dam provide water and energy to millions of people in the southwestern United States. Federal agencies have long acknowledged the possibility of a terrorist attack on this critical Colorado River facility. A serious, deliberate disruption—such as an explosion or radiological contamination—would endanger many lives.

As one example of hydroterrorism, such a threat requires proactive planning and response. In the late 1990s, the Federal Highway Administration began exploring options to redesign U.S. Route 93, which originally crossed Hoover Dam. One purpose of the bypass project was to protect "dam and power plant facilities and the waters of Lake Mead and the Colorado River from hazardous spills or explosions" (FHWA 2001). Approved in early 2001, the bypass project was expedited after the events of 9/11 showed that large-scale domestic terror attacks were possible. The project, with its well-known bridge (Figure 1), was completed in 2010. Dam personnel and local units have trained to respond to a radiological-contamination scenario (DOE 2009), and Hoover Dam police constantly patrol the facility, fulfilling their mission of "safeguarding a

national icon" and "protecting the dam from attack or terroristic threat" (USBR 2015).

Definitions

No formal definition of hydroterrorism yet exists. Like cyberterrorism and bioterrorism, the prefix denotes the tactics used, in this case, water. One may therefore broadly define hydroterrorism as a subset of terrorist activity (i.e., ideologically motivated violence, intimidation, and/or sabotage) in which water is the tool or the target.

The need for a more precise definition is still in question. Considering cyberterrorism, Jarvis and Macdonald (2015) found four different attitudes that influence its many definitions. By the same reasoning, depending on definitions compared to general terrorism, hydroterrorism may be 1) nonexistent, 2) distinct, 3) indistinct, or 4) a distinct subset. A specific definition of hydroterrorism, or terrorism with any other prefix, while potentially useful, may elude immediate consensus.

Still, the broad definition given above will suffice, to be illustrated with several examples described below.

History of Hydroterrorism

Hydroterrorism is not new. A study of history, particularly in warfare and political conflict, reveals several examples (Gleick 2006). One incident dates to about 2400 B.C., when the king of Lagesh diverted water into boundary canals and effectively deprived a neighboring rival kingdom of its water supply. Around 600 B.C., Solon of Athens poisoned the city of Cirrha's water supply, which reportedly sickened the residents and facilitated the city's capture.

Gleick (2006) cited over 50 more-modern instances from 1748 to 2006, most of which had occurred since 1990 (Figure 2). Notable examples include the bombing of a main water pipeline in Baghdad, the destruction of wells in Pakistan, and the withholding of water supplies by rebels in Sri Lanka.

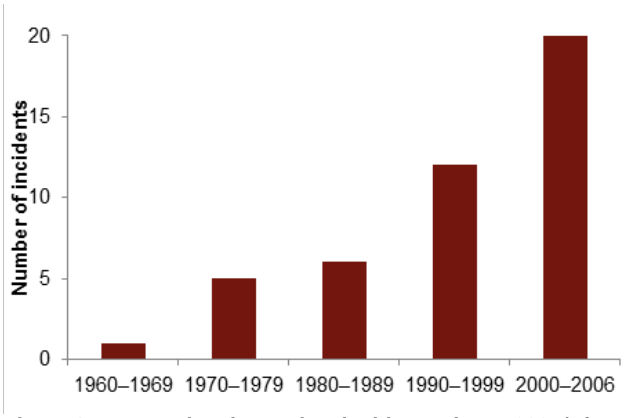

Figure 2: Water-related terrorism incidents since 1960. *(After Gleick 2006)*

Hydroterrorism Today

While historical reports of hydroterrorism are informative, they do not capture the immediate peril. Climate change and regional water scarcity, particularly in the Middle East, appear to be driving more water-related attacks (Ramaswami 2014; Shakdam 2015).

One must only look as far back as last summer to see large-scale hydroterrorism in action. The capture and closure of an Iraqi dam (Figure 3) by ISIS militants in June 2015 underscores the ongoing threat, as reported in the *Guardian* (2015): "Islamic State jihadis have closed the gates of a dam in the Iraqi city of Ramadi that they seized last month, posing a humanitarian and security threat, officials have said. [ISIS] fighters have repeatedly sought to control dams in Iraq, in some cases reducing the flow of water to areas under government control or flooding swathes of land to impede military operations."

Al-Marashi (2015) observed that "the role of water in conflict in the Middle East has existed since time immemorial, but [ISIS] has used it to such an effect that it deserves credit for mastering 'hydro-terrorism,' threatening to flood downstream towns and deprive them of a resource essential for daily survival and irrigation."

The closure also served tactical purposes: "Reducing the water level of the Euphrates granted the group greater freedom of movement to traverse water arteries, facilitating their ability to carry out attacks on government forces on the opposite bank of the Euphrates" (Al-Marashi 2015).

Figure 3: Ramadi, Iraq, with dam at top center. *(Google Earth/ DigitalGlobe)*

In the Middle East in particular, where water is scarce, the trend to "weaponize water—the new tool of terrorism" is growing (Shakdam 2015). Reporting on the incident, CNN called "water the ultimate weapon in this blistering desert" and military analyst Lt. Gen. Mark Hertling (Ret.) said, "there is this belief of if you can control the water, you can control your enemy, which in that part of the world is basically true" (Alkhshali and Smith-Spark 2015).

This is just one recent incident. Lest one think that hydroterrorism is confined to conflict in the Middle East, Gleick (2006) cites scores of other examples worldwide.

Threats

Like other critical infrastructure, water resource systems are potential terror targets. They "have been designed, built, and operated in an open and free society. Thus, they always have been vulnerable to violent acts, including terrorist attacks" (Haimes 2002). Most water resource systems have many centralized and distributed facilities, offering multiple access points for potential attackers. In the past, few stringent security measures were established to protect such systems, though precautions at major U.S. facilities like Hoover Dam have increased in the post-9/11 era.

A terrorist attack could impair, damage, or destroy water infrastructure on a variety of scales. The Department of Homeland Security acknowledged that the nation's 160,000 public drinking water systems, which serve 84% of the U.S. population, are "vulnerable to a variety of attacks, including contamination with deadly agents, physical attacks such as the release of toxic gaseous chemicals, and cyberattacks" (DHS 2016). The EPA (2010) stated that "plausible attack methods include explosive devices; contamination in drinking water distribution systems; sabotage of water treatment systems; hazardous material releases; and cyberattacks." Complete destruction notwithstanding, infrastructure targets may include:

- water sources, which may be contaminated or disrupted;
- water and wastewater treatment works, which may be disrupted by equipment failure, power failure, chemical manipulation, or other means;
- pump stations, which may be disrupted by equipment failure, power failure, or other means;
- storage tanks, which may be contaminated or depleted;
- dams and reservoirs, which may be controlled to hold back or release water in harmful ways;
- hydropower facilities, in which the control of energy resources is desired (Al Amin 2013);
- pipelines, which may be severed, overpressurized, or otherwise impaired; and
- valves and other controls, which may be manipulated to restrict, reroute, or release flows in harmful ways.

In addition to the infrastructure threats, hydroterrorism cascades into effects on public health. Clean water is a vital human need from hydration to waste removal; any denial of drinking water or wastewater services could result in "large numbers of illnesses or casualties" (EPA 2010). Other critical services such as firefighting and healthcare also depend on water resources.

Environmental impacts are another concern. Deliberate flooding or drought may damage sensitive ecosystems, wetlands, and waterways, as well as affect food production. Major river systems, by nature of their size and flux, can effectively spread point-source contaminants over large areas, as the Gold King Mine spill last August, though accidental, so clearly illustrated.

Cybersecurity

While physical attacks are still a risk, water utilities may be even more vulnerable to cyberattacks, both intentional and accidental, through their supervisory control and data acquisition (SCADA) systems (AWWA 2014; Saparia and Ginter 2013; EPA 2012; EPA 2010; Gleick 2006; Haimes 2002; Gellman 2002). Designed with little or no attention to security, SCADA systems may be hacked to achieve the same objectives as physical attacks.

Gellman (2002) reported how Vitek Boden in Queensland, Australia, used a remote computer and radio transmitter to control a wastewater system and release "hundreds of thousands of gallons of putrid sludge" into parks, rivers, and private properties. His illicit activity went undetected for two months before he was arrested during his 46th intrusion. The deliberate spills—avenging Boden's rejection from a local government job—killed marine life, turned rivers black, and stunk unbearably. With his "unlimited command of 300 SCADA nodes governing sewage and drinking water alike," the damage could have been much worse.

In 2002, U.S. analysts found that al Qaeda had been researching SCADA programming instructions that run power, water, transport, and communications grids in the United States and abroad (Gellman 2002). Since much of the technical information is available in online forums, security flaws are well known and "an intruder could use virtual tools to destroy real-world lives and property."

A recent investigation found that over 14,000 U.S. Department of the Interior laptops were not properly secured and were "at high risk of compromise" (OIG 2015). The Department includes the U.S. Geological Survey, the Bureau of Land Management, and the Bureau of Reclamation, which oversees many dams in the western United States. In addition to accessing sensitive data, cybercriminals could use the machines "to gain unauthorized access to the Department's computer networks and systems."

Response

Responses to hydroterrorism and related threats depend on the risk. Some measures may be easy to implement, while others may be impossible because of size, cost, expectations, or other factors. Not all water systems merit the same level of security. While both deliberate and accidental disruptions are possible, a proper risk assessment should precede major planning decisions.

Fundamental practices to reduce risk include the following (AWWA 2014; EPA 2012; EPA 2010; Gleick 2006; Beering 2002; Haimes 2002):

- Limit or deny physical access to facilities.
- Install security lighting, surveillance, and motion detectors at facilities.
- Secure and regularly inventory treatment chemicals.
- Limit access to maps, plans, and sensitive operational information.
- Secure SCADA systems with firewalls and strong passwords. Limit users and their permissions. If possible, separate SCADA systems from the internet.
- Automate monitoring of water quality, water levels, pressures, etc.
- Develop an early warning system to detect contamination events.
- Establish procedures and train for temporary shutdowns.
- Plan a public notification system that leverages social media, local radio, local television, and other disseminators.

Many resources related to these practices are available from the American Society of Civil Engineers, American Water Works Association, U.S. Environmental Protection Agency, U.S. Department of Homeland Security, and other organizations.

Where clear hydroterrorism risks exist, they must be addressed. The best approaches will consider both the probability and the consequences to respond accordingly to protect water resources.

References

Al Amin, Mohammed A. 2013. "Hydropower Resources as Target of Terrorism: Case Study of Selected Water Bodies in Northern Nigeria." *The International Journal of Engineering and Science* 2 (11): 52–61.

Al-Marashi, Ibrahim. 2015. "The Dawning of Hydro-Terrorism." *Al Jazeera*, June 19.

Alkhshali, Hamdi, and Laura Smith-Spark. 2015. "Iraq: ISIS Fighters Close Ramadi Dam Gates, Cut Off Water to Loyalist Towns." CNN, June 4.

AWWA (American Water Works Association). 2014. *Process Control System Security Guidance for the Water Sector*. Washington, D.C.: AWWA Government Affairs Office.

Beering, Peter S. 2002. "Threats on Tap: Understanding the Terrorist Threat to Water." *Journal of Water Resources Planning and Management* 128 (3): 163–167.

DHS (U.S. Department of Homeland Security). 2016. "Water and Wastewater Systems Sector." Critical Infrastructure Sectors. Last updated Jan. 8. http://www.dhs.gov/water-and-wastewater-systems-sector.

DOE (U.S. Department of Energy). 2009. "Hoover Dam Drill Focuses on Terror Threats." *SiteLines* 138 (July/August).

EPA (U.S. Environmental Protection Agency). 2010. *Water Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan.* EPA 817-R-10-001. Office of Ground Water and Drinking Water, Water Security Division.

———. 2012. "Cyber Security 101 for Water Utilities." EPA 817-K-12-004. Office of Water.

FHWA (Federal Highway Administration). 2001. *U.S. 93 Hoover Dam Bypass Project: Final Environmental Impact Statement and Section 4(f) Evaluation, Volume I.* FHWA-AZNV-EIS-98-03-F.

Gellman, Barton. 2002. "Cyber-Attacks by Al Qaeda Feared." *The Washington Post*, June 27.

Gleick, Peter H. 2006. "Water and Terrorism." *Water Policy* 8 (6): 481–503.

Guardian. 2015. "Isis Closes Ramadi Dam Gates, Cutting off Water to Pro-government Towns." *The Guardian*, June 2.

Haimes, Yacov Y. 2002. "Strategic Responses to Risks of Terrorism to Water Resources." *Journal of Water Resources Planning and Management* 128 (6): 383–389.

Jarvis, Lee, and Stuart Macdonald. 2015. "What Is Cyberterrorism? Findings from a Survey of Researchers." *Terrorism and Political Violence* 27 (4): 657–678.

OIG (Office of the Inspector General). 2015. "Management Advisory – Failure to Adequately Protect Sensitive Data on Thousands of U.S. Department of the Interior Laptop Computers." Report No. ISD-IN-MOA-0004-2014-H. U.S. Department of the Interior. Memorandum, Dec. 21.

Ramaswami, Abhishek. 2014. "Water Terrorism: How Militant Groups Are Taking Advantage of Climate Change Impacts." *Breaking Energy*, Dec. 9.

Sandia National Laboratories. 2001. "Two New Methodologies Can Help Owners Improve Security of Nation's Dams and Power Systems." News release, Dec. 10. http://www.sandia.gov/media/NewsRel/NR2001/ramdramt.htm.

Saparia, Biren, and Andrew Ginter. 2013. "Restricted Access: Detroit Water's Operational Data Area Both Protected and Accessible with Unidirectional Security Gateways." *Water Environment & Technology* 25 (6): 56–59.

Shakdam, Catherine. 2015. "Vying for Control over Water: Why ISIS' Grand Ambitions Put Everyone at Risk." RT, June 10.

USBR (U.S. Bureau of Reclamation). 2015. "About Us." Hoover Dam Police Department. Last updated Mar. 19. http://www.usbr.gov/lc/hooverdam/police/aboutus.html.