Catalan autonomous police officers descend into a sewage tunnel in routine anti-terrorist patrols

Picture credit: Getty

WATER SECTOR SECURITY

Catherine Laug *examines potential threats and the importance of hi-tech solutions*

The National Critical Infrastructure Protection Plan, a document that unifies a nation's energy, nuclear, finance, transport and water sectors identifies the very real threat our world faces from terrorism.

Although it is not the only threat facing our global infrastructure, terrorism is unfortunately a very topical one, which must be taken seriously. For instance, Spain was recently placed on Terrorist Alert Level 4 (with the lowest level being 1 and the highest being 5). One area frequently unheeded by citizens, however, is the genuine risk to our water infrastructure. But why?

Faced with a terrorist attack, the population tends to contextualise the situation in order to protect itself. In most cases attacks are seen as abstract, affecting others in relatively remote locations. However, if it happens in the same city, in a very busy place to something like public transport, the psychological effect on the population is much greater and this is the main effect sought by terrorists: to create a feeling of insecurity in individuals.

In the case of water, the consequences of an attack on the water infrastructure would extend to homes, where everyone feels most secure. Added to this is the fact that an attack of this nature is initially undetectable by the population.

Recent studies undertaken by the United States Air Force and Colorado State University reveal that a few litres of a highly toxic substance is sufficient to pollute an entire food system of a population of 100,000 people in just a few hours. But where are the vulnerabilities in the system?

There are many different water sources, including reservoirs, rivers, streams, lakes, deep wells, underground water from wells fed by surface water and desalination or waste water treatment plants. The solution against pollution is dilution. In addition, many of the potential pollutants degrade over time by exposure to the sun and the elements, giving these sources a self-cleaning character that makes them difficult, but not impossible to contaminate.

DRINKING WATER VULNERABILITIES

However an attack on the drinking water system can take a variety of forms as the supply of water to our homes is a complex process, involving many different steps, all of which are to some extent vulnerable to terrorist acts and need securing. These include:

Processing plants: In the majority of cases, the treatment plant constitutes the last bulwark between pollution (natural, accidental or intentional) and the end user. Often, it is also the last place of continuous control of the chemical and physical characteristics of water.

Water reservoirs: These sites, such as treatment plants, are places with limited geographical space and can thus benefit from a certain level of physical security. They are often found in remote areas, and are widely dispersed, so monitoring can be insufficient in places. The volume of water involved is also reduced, but there is still some potential for dilution.

The distribution system: It is generally accepted that the distribution system is the most vulnerable element of the water supply system. The dilution potential is considerably reduced. The most likely scenario for an attack whose purpose is to inflict serious fatal damage is to organise reflux contamination. A reflux attack occurs when a pump is used to exceed the pressure gradient present in the pipes of the distribution system.

A large number of different toxic compounds can be deployed by terrorists in an attack on water resources and these include:

Chemical compounds used for water treatment: These compounds, such as chlorine or fluoride – which improve the quality of water used in adequate doses – can become toxic in excessive amounts. These chemicals are readily available because they are present in the facilities and improper handling, either intentional or accidental, can have serious consequences. In addition, automated systems can be subject to cyber attacks and can cause damage from thousands of kilometres away.

Heavy metals: These are hazardous because of their toxicity to humans. They are also fairly simple to obtain, and their salts often dissolve easily.

Herbicides: In general, herbicides tend to be less harmful to humans than other compounds, although there are some notable exceptions. However, it is very easy to obtain these in large quantities, which increases the risk of use. Although not causing a very high death toll, the panic engendered by their presence in distribution networks could be serious.

Insecticides: These are generally more harmful to humans than herbicides. Some insecticides have chemical structures very similar to certain chemical warfare agents. Like herbicides, insecticides are available in large quantities. For some, their solubility limits their effectiveness as weapons when introduced into water, but others are very soluble and pose a threat.

Nematocides and rodenticides: Nematocides are similar to insecticides. With few exceptions, they are more soluble than insecticides. Some nematocidal compounds are also similar to chemical warfare agents because of their structure and mode of action. Rodenticides are of concern because they are specifically designed to be fatal to certain species of mammals such as humans. Both types of products are available in large quantities.

Industrial chemicals and miscellaneous agents: There is an abundance of industrial chemicals that could be used for attack. Their main representative is cyanide, which is widely used in mining and other industries.

Radionuclides: The use of radionuclides as a weapon is a highly probable risk. Even with limited casualties, the psychological impact of a radiological threat could be severe. Highly pure compounds and highly radioactive materials such as plutonium or uranium-238 are difficult to procure and expensive, and it is unlikely that a terrorist organisation that has acquired these materials will be willing to use them for an attack on a water supply system. The use of low-level radioactive materials or residues is more likely.

War Agents: Chemical warfare agents like VX, soman, sarin or mustard gas aren't normally used because of their limited availability. If used for an attack, it is more likely to be aerosolised.

DELIVERING A ROBUST AND FULLY TRACEABLE ACCESS CONTROL SOLUTION IS ESSENTIAL

Toxins and biological agents: There are a number of protozoa, bacteria, viruses and toxins that could be used in an attack. Many of these agents are extremely toxic and contain compounds such as botulinum toxin, which is one of the most toxic substances known. These categories of products are fairly easy to obtain and examples of castor production by terrorists are not lacking. Bacteria are also easily cultivable and wastewater could in fact be used as a potential pollutant for a reflux attack.

A contamination would not be confined to areas near the point of introduction, as the pollutant would quickly flow through the entire neighbourhood accessing major pipelines, leading to the pollution of the entire system.

CRUNCHING THE NUMBERS

Computer simulations have demonstrated that by using a military agent to attack the nervous system, more than 20 percent of the population would receive a dose sufficient to cause death and, with a common chemical agent, the result would exceed 10 percent.

Significantly, calculations revealed that this type of attack could be organised for less than four pence per death. Thus, considerable damage can be committed at a very low cost and by means of a very simple technology.

An attack on water resources undoubtedly satisfies the terrorist criteria, as outlined by the 9/11 Commission, which concluded that al Qaeda uses specific criteria to plan an attack and access the effectiveness of a mission.

This is not a hypothesis but a very real threat to every nation, with historical evidence of attacks on water resources being played out throughout history. Records as early as 1000 BC reveal Chinese warriors contaminated the water resources of their enemies with arsenic. While not exhaustive, there have been recently documented incidents too, including the arrest of four men of the Salafist Group for Preaching and Combat (GSPC) who were arrested in Rome for possession of chemicals, false papers and detailed plans for the water supply network in the zone of the Embassy of the United States.

FIRST LINE OF DEFENCE

The first line of defence against an attack of this nature is prevention, in order to prevent the attack from occurring. If prevention fails or is impossible, the next strategy is to detect the presence of pollutants in the water before they reach the population. For this, the best solution consists of multi-parameter probes of continuous analysis, which measure the usual parameters of water quality and then look for the anomalies that may indicate the presence of a contamination. These sensors include parameters such as chlorine, total organic carbon, pH, conductivity, turbidity, UV absorbance/fluorescence. One of the advantages of this approach is that it uses widely available instruments commonly used to perform such analyses.

An attack on the drinking water system can take a variety of forms as the supply to our homes is a complex process involving many different steps, from reservoirs to processing plants, and all are to some extent vulnerable to terrorist acts.

As always, the first line of defence against any attack is prevention, particularly physically securing our water infrastructure and prohibiting unauthorised access to these sites. With many sites isolated and manned by countless personnel across an entire region, delivering a robust and fully traceable access control solution is essential. With the ability to carry out audits and respond quickly to new technologies, through fixed terminals or mobile apps, electronic key-centric access management provides users with complete control over entire regional sites. They can receive up-to-the-minute information about all events relating to access – which can enable them to adjust user profiles centrally while the users will be given access locally thanks to their Bluetooth Key and App for instance.

CONSIDERABLE DAMAGE CAN BE COMMITTED AT A VERY LOW COST AND WITH VERY SIMPLE TECHNOLOGY

In conclusion, while even the slightest hint of terrorism is always alarming, it may be the least risky threat to our water infrastructure. However, given the potential risk an act of this nature could deliver, it is necessary to be prepared and secure our sources now. With approximately 6.5 billion cubic metres of water directly abstracted for public use in England and Wales each year alone, securing and controlling access to drinking water sites is of critical importance ●

Catherine Laug is the Marketing & Communications Manager for Locken. A provider of digital access control solutions, Locken delivers innovative access management and increased security to large, single-site companies and multi-site businesses. Responsible for defining and executing the corporate marketing strategy across Locken's key European territories, Catherine's remit also covers the UK division – Locken UK Ltd.

A meaningful way to control who can access water works is vital

Picture credit: Locken UK Ltd.