



Articles

Water Critical Infrastructure Security and Its Dependencies

by David Michael Birkett



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

Abstract

Water critical infrastructure (CI) is considered one of the most important CI on a global basis. Indeed, the average person is only able to survive for 3 days without water. Water CI has been consistently targeted across history since 3000 BC, with a significant increase in those attacks documented in the early 2010s. The aim of this paper is to review security and dependencies of water CI in relation to adverse human intervention. In particular, the paper analyses water as a 'soft' target, and provides an insight into terrorist attack planning and perceived threat levels. It is concluded that the lack of clear understanding of dependencies and interdependencies can lead to an increase of water CI vulnerability, which could, in case of external attack, result in a sudden and protracted cascading failure. Development of future partnerships and linkages across the supply chains could increase awareness of potential failures, which may assist in a reduction of any future potential impacts. Finally, water CI is recognised as a terrorist target. Hardening water CI protection is necessary, and is required to be regularly assessed and hardened against external adverse human intervention, such as terrorism, in order to inhibit its future selection as a target of a terrorist attack.

Keywords: *Water critical infrastructure; security; terrorist attack; dependency; water contamination*

1 Introduction

Water and wastewater critical infrastructure (CI) (further referred to only as water CI) is considered essential for contemporary social human existence (Cohen, 2010, Lee, 2009b). Water CI, with the technology required to run and operate on a daily basis, is considered to be amongst the most critical of CIs. The importance and criticality of water CI is validated, as it is generally agreed that water is (just after air) the most precious commodity for humankind to survive (Cohen, 2010, Lee, 2009b). Cohen and Lee confirm that the average person is only able to survive three days without the intake of water to maintain the human body systems health and functionality. Moreover, modern society relies heavily on the unseen operation of the removal and disposal of human waste through the wastewater systems as a form of essential CI that ensures the separation of treated drinking water and faecal contamination from human waste. This separation reduces the potential for community outbreaks of waterborne diseases, as occurred in the cholera outbreak in London prior to 1857 (Snow, 1857). Consequently, adequately treated water supplies and wastewater services are essential for society expectations, global development and human health.

The demand for water resources is increasing relative to the demographic pressures of population growth, with the primary water resources remaining static or diminishing across multiple countries (Wolf, 2007). The identified reduced per capita water availability is based on predictive population increases, combined with an anticipated increase in living standards within the individual countries, resulting in an increase in water



consumption (Pimentel et al., 1997). (Wolf, 2007) advises further that due to resource neglect, on a global basis, both water quantity and quality have deteriorated to the point of catastrophe, with:

- A billion people, or more, globally, lacking access to safe water supplies
- Almost three billion lack access to adequate sanitation
- An estimated five to ten billion people die each year from water related disease or inadequate sanitation
- Twenty percent of the world's irrigated lands have become salt laden, affecting agricultural production

The criticality of water infrastructure in relation to a potential terrorist attack has become increasingly significant with the growth of world population in the 20th and 21st centuries (Gilbert et al., 2003) placing increased demands on water sources. This criticality, coupled with the complexity and extension of water supply chains within an environment of climate change and the phenomena of extreme weather fluctuations, again highlights future water scarcity, and potentially further impacts the precarious global food-water nexus balance (Khan and Hanjra, 2009).

Water is predicted to be in shorter supply by 2025, in consideration of the projected global population increases, coupled with forecasted increases in water consumption by individual countries (Gleick, 1993). Gleick also advises that hydrologists have identified that the minimum water requirement for each person residing in an efficient, modern, industrialised nation is 1,000 cubic metres of water per day, or 50 litres of water, per person, per day (Gleick, 1996). There are 32 countries identified by Gleick to be deficient in water resources, requiring some future innovative water sustainability initiatives (Gleick, 1993). This anticipated deficiency raises the profile of water as a more valuable resource, and increases the likelihood of potential adverse human intervention to drinking water supplies. Furthermore, this designated deficiency tends to elevate the value of water to a terrorist group (Gleick, 1993), identifying water as a vulnerable target for potential terrorist attacks (Gleick, 2006) (Kroll, 2006) (Brockett, 2015).

This paper discusses the security of water CI in relation to adverse human interventions. It also additionally discusses the dependencies of water CI, relative to other CI, which may potentially, create a cascading series of failures across industry within the broader industrial economy. Furthermore, how in a water industry context these dependencies may affect the water service delivery, subject to any unplanned interruptions in the existing supply chain. The paper has the following structure. Section 2 provides a background containing the history of attacks on water CI and conflicts in water supply, as well as contamination of water supply. Section 3 reviews dependencies of water CI, including dependencies of other CIs on water and risks of those dependencies. Section 4 analyses the security of water CI and its perceived threats in relation to a terrorist attack. This section represents the main contribution of this paper in the areas of assessing water CI as a 'soft' target and a description of terrorist attack planning on water CI. Section 5 concludes the paper.

2 Background

2.1 History of attacks on water CI

There are many historical examples of attacks and attempted attacks on water CI (Haines et al., 1998) (Hickman, 1999) (Dick, 2001) (Dreazen, 2001). As indicated in Figure 1, (Gleick and Heberger, 2014) advises that there were 162 documented attacks on water CI from 1980 to 2012, with a measured increase from 1970



to 2000. Gleick et al (2014) documents a sudden rise up to 31 attacks in a 12 month period in 2012 (Gleick and Heberger, 2014). Although (Gleick and Heberger, 2014) documents attacks on water since 3000 BC there is an observed increase in attacks since 1998. However, it may be considered that in the perspective of increased modern media technology and improved monitoring systems in contrast with the lack of communications historically, that there may well have been a higher number of incidents in earlier history than is apparent from the records currently available.

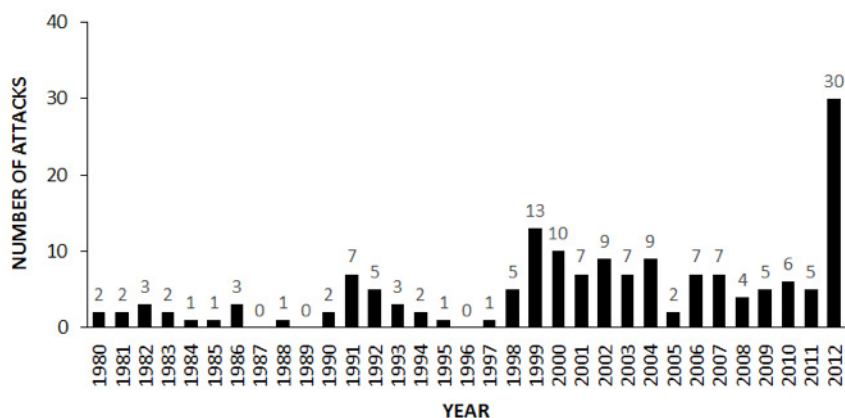


Figure 1: Recorded attacks on water critical infrastructure (adapted from (Abrams and Weiss, 2008, Gleick and Heberger, 2014, Kroll, 2010, Weiss, 2011))

Furthermore, in recent times, there is an observed increased level of interest in attacks on water CI displayed by Jihadist terrorist groups, such as al Qaeda and others. This interest is evident from documents and computer records retrieved by Western Intelligence Agencies and Law Enforcement (Kroll, 2012b) (Brockett, 2015). Amongst documented examples are the attempted terrorist contamination of drinking water in Rome (Kroll, 2012b) (Balmer, 2004), Cyber hackers attacking U.S. water systems (Weiss, 2011), an attempted water poisoning in Spain linked to al-Qaeda (Silva, 2011) and Iraq insurgents using water as a weapon (Coles, 2014). Recorded examples from Australia in 1984 (Noble and Schrembi, 1984) and in 2012 (ABC, 2003) are two separate incidents connected with a terrorist act. associated with threats to poison water supplies (Cooper, 2013).

2.2 History of conflict in water supply

The application of deliberate adverse human contamination of water, as a form of military or aggressive attack by nation States or disparate terrorist groups is not a new or modern phenomena, and is evident over a long historical timeline (Kroll, 2006). Indeed (Wolf et al., 2005) documents that rivalries over shared use of water has existed since the Neolithic revolution with the human race settling to cultivate food between 8000 and 6000 BC. The term ‘rivalry’ originates from the Latin word ‘*rivalis*’ meaning “one using the same river as another” (Wolf et al., 2005). Inter country disputes and rivalry over water is evident today between downstream and upstream users, such as Syria about Turkey; Pakistan about India and Egypt regarding Ethiopia (Wolf et al., 2005). Examples and case studies of water conflicts are many since 3000 BC, with Gleick et al detailing 265 incidents to 2012 (Gleick and Heberger, 2014), and Kroll documenting 63 incidents selected between 1000 BC and 2005 (Kroll, 2006). A few selected incidents of the use of water as a weapon between nations and external groups, as distinct to deliberate contamination by an internal terrorist group, are as follows:



- In 1939 The Japanese military poisoned Soviet water sources with intestinal typhoid bacteria in an area near the former Mongolian border (Kroll, 2010).
- In the period 1939 to 1942 the Japanese military 'Unit 731' poisoned Chinese water sources, wells and bulk water storages with typhoid and other Chemical and biological pathogens (Gleick and Heberger, 2014).
- In November 1944, Soviet troops flooded the area south of the Istra Reservoir near Moscow, Russia. This was a strategy to slow the German advance on Moscow. A few weeks later, German troops used the same tactic to create a water barrier to halt advances by the Soviet 16th Army (Gleick and Heberger, 2014).
- In 1945 The Desperate and retreating German Army poisoned a large reservoir in Bohemia with raw sewage (Kroll, 2010).
- In 1965 Yasir Arafat's Fatah movement orchestrated several bombing attacks on Israeli water infrastructure. The Fatah movement was also responsible for additional attacks on Israeli water pipes (Kroll, 2010).
- In July 2002 U.S. Federal officials, in Denver, arrested two al Qaeda operatives in possession of documents detailing how to poison the country's water supplies (Kroll, 2010).
- In 2004, In the U.S. 50 unwanted water system intrusion incidents were identified by 10 federal agencies involving SCADA computer systems that control water supply and wastewater systems (Gleick and Heberger, 2014) (Kroll, 2006).
- In 2002, Italian Police arrested 4 Moroccans, with links to al-Qaeda, allegedly planning to contaminate a section of the Rome, Italy, drinking water supply with a cyanide – based chemical ; (Gleick and Heberger, 2014, Kroll, 2006).

As indicated water is a historically regarded as a useful weapon to terrorise populations and kill large numbers of populations for various political and strategic motivations. As (Gleick, 1993) indicates,

“As we approach the twenty-first century, water and water-supply systems are increasingly likely to be both objectives of military action and instruments of war as human populations grow, as improving standards of living increase the demand for fresh water, and as global climatic changes make water supply and demand more problematic and uncertain” [1]

Indeed, the future global availability of drinking waters are considered at risk and furthermore is considered a significant international problem, with competition between countries and regions continuing to grow. This places political pressures on the future supply of water (Pimentel et al., 1997) and increases the potential risk exposure of future water of acts of terrorism.

The potential for terrorism was also recognised in 1941, during the Second World War, when Federal Bureau of Investigation (FBI) Director J. Edgar Hoover wrote,

“It has long been recognized that 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” (Copeland and Cody, 2003).

In consideration of the easy access to the required technical knowledge of water single points of failure (SPOF) and the availability of relevant toxins, with additional considerations of the ease of global internet



access, water contamination incidents affecting large populations may well increase as a future form of terrorism targeting, and selection transference, as other current popular targets harden. The chance or likelihood of terrorists targeting water is certainly very real (Gleick, 2006) (Dreazen, 2001) (Beering, 2002) (Cameron, 2002) (AAP, 2003). Water infrastructure may be targeted directly to damage water processing or delivery systems, or alternatively water may be contaminated through the introduction of poison or disease causing pathogens or chemicals within the water distribution systems as a form of 'backflow' (Kroll et al., 2010b).

2.3 Contamination of water supply and response

Many current instances of water related incidents indicate that the primary first notifications of any deliberate (or even accidental) water contamination would probably originate from the health sector, such as occurred in May 2015 in Prague, Czech Republic, which is discussed in more detail further within this paper (Willoughby, 2015) & (Lazarova, 2015). Furthermore, Meinhardt suggests that medical training and education for this type of event may well be deficient (Meinhardt, 2006). Internationally, most historically based water security measures are primarily concerned with detecting and responding to water quality, subsequent to variations in water parameters, such as pressure of supply, filtration and chlorination as effective treatment techniques for protecting water supplies (Cook and Bakker, 2012, CRC, 2008, E.P.A., 2000, Ireland, 2011, Schutte, 2006). Furthermore, (Palaniappan et al., 2010) considers that on an international basis, contamination by natural pathogenic organisms, trace metals, industrial toxic chemicals and changes in the acidity, temperature and salinity of water are more significant issues of concern. These traditional measurements of water quality monitoring may not be effective in identifying deliberate adverse human intervention with the introduction of harmful pathogens or chemicals. Detection sensors have been developed to detect this form of contamination (Kroll, 2008) & (Brockett, 2015) by various international groups. However, sensor detectors are not installed in all locations across water systems, and are potentially expensive for water entities to install on all parts of the water network.

A medically reported example of contamination by human error in 1988 was the accidental discharge of 20 tonnes of aluminium sulphate into the treated water reservoir that supplied treated water to the Camelford area of Cornwall in the United Kingdom. The water was heavily contaminated with aluminium with a low pH. With an extensive delay in identifying the contamination from testing, a significant community increase of rashes and gastrointestinal disturbances occurred within a few days, and later cases of musculoskeletal pains, malaise and impairment of concentration and memory. Subsequent to the medical alert of this incident, two years later approximately 400 persons were reported as still suffering from symptoms that they attribute to this incident (Altman et al., 2006, BBC and Rose, 2012, Morris, 2012, Reid, 2007).

As previously mentioned, an example which supports Meinhardt's medical hypothesis related to water contamination, is the reported contamination in the city of Prague, Czech Republic (Willoughby, 2015). This incident was initially reported by the Prague health services on Friday 22 May 2015 (Lazarova, 2015). Public notification was advised by the utility on Sunday 24th May 2015 (Willoughby, 2015), as 250 people were admitted to hospital with severe symptoms as a consequence of contamination from coliform bacteria and norovirus in the water distribution system (Monitor, 2015a, Monitor, 2015b). In consideration of the nominal 2-3 days bacterial incubation period of coliform bacteria, the water distribution system would possibly have been contaminated on Tuesday 19th May, or Wednesday 20th May 2015 (Turcios et al., 2006). The 320,000 inhabitants were advised to not drink the water and water tanks were supplied for people to



safely drink (Willoughby, 2015). The pathogen was identified as ‘e-coli’ and ‘Norovirus’, and believed to be a naturally occurring pathogen contaminating the water system (Monitor, 2015a). The primary identification of the water born pathogen appeared to be from the health services, prior to water contamination monitoring from regulatory sources. The May 2015 Prague contamination incident is perhaps a reflection of reality, that prior to any deliberate contamination being recognised by scientific or technological assessment, people may be deceased or ill, with the primary alert issued from medical services (Meinhardt, 2005). Prague 6, the identified region of this contamination is the area where most foreign missions and embassies are located in Prague.

Craig Stanners recently expressed some concerns over deliberate water contamination in the U.K. in the U.K. media, with an observed absence of water monitoring. As Director of IVL Flow Control in the U.K., Stanners stated that, “The UK’s drinking water is at far too great a risk from potential contamination of supply by terrorists, with current systems simply not quick enough to contain a chemical or biological attack” (Brockett, 2015) and “What’s in place at the moment isn’t anywhere near quick enough to cope,” said Stanners. “Those wishing to cause damage to our drinking water would laugh at our response that we’re waiting five days for results to come back from the lab—by then, it will be too late” (Brockett, 2015). Stanners also cited previous Al-Queda threats to poison drinking water in American and Western cities, in addition to arrests in Jordan of Iraqi agents who attempted to poison the water supply that served American troops in the eastern Jordanian desert (Feuer, 2003).

However, (Gleick, 2006) suggests that it is not necessary to contaminate water supplies, with the terrorist objective achieved by a plausible threat to contaminate. The mild ingress of a harmless vegetable dye would potentially be sufficient to create the sought objective of fear and chaos in the community.

3 Dependencies of water critical infrastructure

The continual progression of the computerisation of modern society, relative to critical infrastructure, has created an expanding incremental dovetailing of complex and increasingly dependent linkages across the value chain of each critical infrastructure (Figure 2). Gillette expands on these increasingly complex linkage vulnerabilities by computer and utility communications.

“Mutual dependence and interconnectedness made possible by the information and communications infrastructure lead to the possibility that our infrastructures may be vulnerable in ways they never have been before” (Gillette et al., 2002).

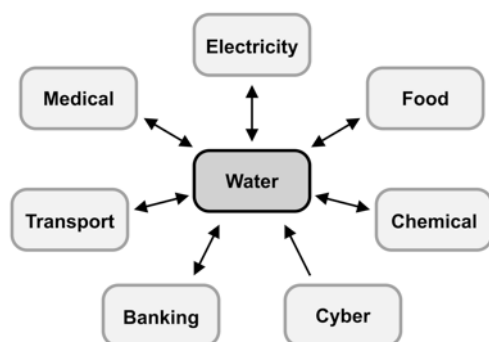


Figure 2: *Dependency of water critical infrastructure on other CIs*

The dependency of water infrastructure firstly to water CI’s supply chain and secondly to other forms of CI is



a significant issue for water managers. An example of the complexity of these dependent relationships is that water CI displays a strong reliance on the chemical industry CI to perform disinfection and water treatment. The chemicals are conveyed, and delivered, by the transport CI sector to water CI destinations, utilising rail, road and marine transport. In a hypothetical case of the various key assets of the transport sector being compromised as a consequence of a terrorist attack, the chemical CI may not be delivered, the transport sector may not function and the water CI may well cease to deliver products and services (Bennett, 2007). In addition to the challenge of potential full outages of various dependent CI as described, emerges one of the most significant business questions relating to interdependency interruptions to Water CI service delivery. That is the issue of service outage time prior to restoration of service or product to maintain the operability of the water service to customers (Gillette et al., 2002)

To a certain extent, restoration times are identified, assessed and analysed, within industry business continuity plans (BCP) to effectively maintain the activities of the specific business. Indeed, (Bouwman et al., 2006) consider that the growing trend of the increasing connectivity between infrastructures and the interdependent services creates new vulnerabilities to be considered. Furthermore, it is suggested that targeted attacks on vital points or identified SPOFs[2] within the water dependent supply chain, may well cripple water CI delivery. This action, directed at the water sector supply chain, may well create a series of interconnected infrastructure failures, which consequently may subsequently influence water CI service outage time.

Water distribution systems have grown exponentially, relative to the growth of the economy and with consideration to population spread across geographical areas. However, over the recent decade the dependent and interdependent technological value chain has sustained a period of growth and extension to support the industry. Furthermore, (Gillette et al., 2002) warns that:

“Failure to understand how disruptions to one infrastructure could cascade to others, exacerbate response and recovery efforts, or result in common cause failures leaves planners, operators, and emergency response personnel unprepared to deal effectively with the impacts of such disruptions.”

It is this perception of the failure to understand these often hidden dependence and interdependency nodes, which may affect the water sector suddenly, with minimal warning, and may well escalate to contribute to a series of cascading failures across other interdependent infrastructure.

3.1 Dependencies of other critical infrastructures on water

The service chain dependency of water is understood to be the most significant reliance of any CI on water and wastewater to continue to conduct normal business. (Sullivan, 2011) considers that most CI sectors are to a certain extent dependent on the water sector. According to (Porod et al., 2014) the water CI sector interconnects strongly with all other CI, and in a recent survey, 75% of all U.S. CI could be directly impacted should the continuous supply of treated water be lost. This dependency can lead to major incremental cascading effects across societies in the case of a sudden absence of treated water and wastewater services. (Porod et al., 2014) identifies that most other CI display a dependency on water services varying in a percentage from 67%–99% reduction in service loss, after 4 hours of water loss. Additionally, critical manufacturing, after a six-hour period of wastewater loss, is predicted to experience a 34%–66% reduction in production.

A dependency analysis conducted by (Porod et al., 2014) across 12 identified CI areas, related the specific CIs



to their dependency to water by percentage of dependency, and estimated offline degradation time without a water supply. Of specific interest to the issue of water vulnerability, as separate from the actual mitigation of the water distribution system itself, is the aspect of interdependency, which is in the form of the mutual dependency of water with other CI. An example of this is the electricity CI displaying a 92% dependency on water, with a 4-hour degradation period (Porod, 2014). The interdependency of water is reflected in the use of water within the generation plant's cooling systems, with the continued supply of electricity essential for water supply pumps, water and wastewater treatment processes and the SCADA communications network for the remote operation of the water and Wastewater network.

Furthermore, as the water industry progressively attains a greater dependency on computers, the supply chain vulnerabilities are increasingly hidden within the context of an assumed product or service supply. To a certain extent, these SPOFs may be forgotten, overlooked or neglected during water vulnerability assessments. Although water and wastewater are considered essential, to varying degrees, on a wide variety of other CIs, water is also dependent, displaying an interdependency of varying percentages. Electricity is considered as an essential form of CI dependency for water and wastewater, to supply pumps, treatment and operational controls, as is the CI of chemicals to treat the water and wastewater. It is these often-variable interdependencies and dependencies, which are considered the 'soft underbelly' of water, displaying the often-overlooked single points of failure, without which the water or wastewater service may not operate effectively.

3.2 Risk of dependencies

The challenge of analysing the risk or threat perception of interconnected interdependent systems of infrastructure is becoming increasingly complex as modern society and technology progresses, with computerised automated ordering systems reflecting variances in individual risk exposures and resistance to service failures (Brown et al., 2004). However, some researchers have developed tools and processes to assess this arduous task, such as (Brown et al., 2004), who describe the goal of assessing the "complex adaptive systems" as identifying the significant risks to critical systems and devising effective mechanisms for mitigating these risks. A suite of simulation tools have been developed at Sandia National Laboratories in the United States, utilising a systems viewpoint and analysis techniques (Brown et al., 2004).

(Brown et al., 2004) describes a generic process, which may be applied to water CI when evaluating the risks inherent in the identified supply chain to clarify the potential risks from either adverse human intervention or on an all hazard basis, the natural risks and threats, which may affect or imping on the supply chain service delivery. Many other forms of analysis and mitigation processes have been developed to assess the vulnerabilities of the supply chain vulnerabilities and CI, with some incorporating algorithmic analysis and assessment (Brown et al., 2004, Hokstad et al., 2012, Rinaldi, 2004). However, as Rudner states :

"While actuarial risks (e.g. accidents, criminal acts, fire) can be assessed quite conventionally through insurance-type risk assignment and risk-sharing principles, the evaluation of terrorism risk presents significantly more problematic challenges to the techniques of risk management:" (Ranstorp, 2007).

The incidence and timing of a terrorist act is less predictable than many of the risks traditionally considered within the spectrum of a risk management matrix.

Nevertheless, in order to adequately comprehend current risk exposures within the spectrum of water and wastewater CI, the system requires to be considered from the broader perspective. To be more concise, an



analysis of the supply chain, in conjunction with the dependent services and industries is required to be undertaken to completely understand the vulnerabilities and threats to service functionality and integrity. The potential water and wastewater subliminal failure and associated predictive industry degradation may be considered in relation to the complexities and number of reliant interdependent services within the supply chain.

Water and wastewater CI may be impacted by multiple and variable dependencies and interdependencies as an indication of the progressive complexities of modern supply chains and interconnected services. Moreover, these dependencies and interdependencies are not currently entirely understood or identified by industry. This perceived lack of understanding may lead to potential significant points of failure in times of disaster or emergency situations. Frequently, their owners or water resilience strategies do not consider these interdependent services and products in their entirety. This lack of clear understanding can lead to a softening of the vulnerability of water and wastewater CI to sudden and protracted failure, particularly from external adverse human intervention.

As these rising levels and complexities of dependent linkages become increasingly dependent on each other, it is often difficult to identify the potential SPOFs that may occur should one of these supportive link nodes fail, with subsequent potential cascading impact on the operation of various critical infrastructure. However, it is the hidden interdependencies and dependencies within the water supply chain, which are becoming increasingly complex and hidden as technology and the computerisation of society progresses. It is this supply chain, which displays the most significant vulnerability for water, which may elude and escape the water, business continuity analysis, and process.

Future partnerships and communications linkages across the supply chain may be developed to discuss and increase awareness of the mutually dependent relationships. These improved relationships would tend to reduce the potential impact of any supply chain failure, and conversely to raise the awareness of the impact of possible water loss on other CI and supply chain owners.

4 Security of water critical infrastructure

4.1 Water critical infrastructure as a 'soft' target

Numerous studies indicate that water CIs are recognised as vulnerable soft targets (Drake, 1998). These studies are related to deliberate, adverse human intervention under the categories of sabotage, terrorism or criminal incidents (Abrams and Weiss, 2008, Birkett et al., 2011, Birkett and Mala-Jetmarova, 2014, Brockett, 2015, Cameron, 2002, Coleman, 2005, Copeland, 2010, Covert, 2008, Kroll, 2010, Gleick, 1993, Kroll, 2006). Furthermore, (Gleick, 1993) comments that as our civilization and development progresses forward in the 21st century, the likelihood of both military action and instruments of war is increasing to involve water and wastewater. He further suggests that as time is progressing in the 21st century, water services are increasingly likely to be the targets of military or aggressive actions.

In consideration of the previous studies indicative of the elevated level of probability of a terrorist attack on water CI, as a soft target, it is appropriate to examine the likely high risk bandings of water CI. As indicated in Figure 3 below, the graded threat bandings may be assessed, and divided into three specific groups, primary, secondary and tertiary. The primary group displays water systems (treated or non-treated). The second radial banding displays the diagrammatic representation of wastewater systems. The tertiary grouping consists of



other ancillary support system functions such as skilled human resources, buildings and facilities, vehicles and equipment, information technology and financial systems. As indicated, the physical and chemical, biological, radiological, nuclear (CBRN) attacks are the most probable, with cyber-attack, supervisory control and data acquisition (SCADA) having an elevated risk in relation to financial and operational control systems. However, all the indicated bandings represent potential terrorist targets in water CI, with terrorist groups potentially identifying the single points of failure (SPOFs).

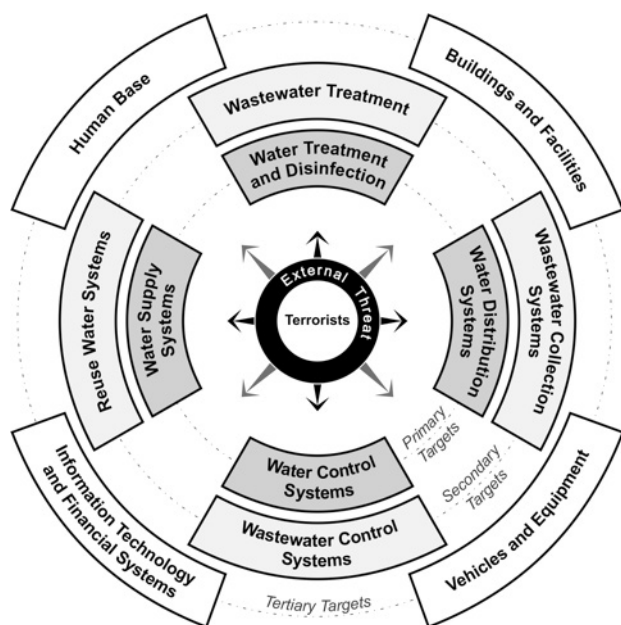
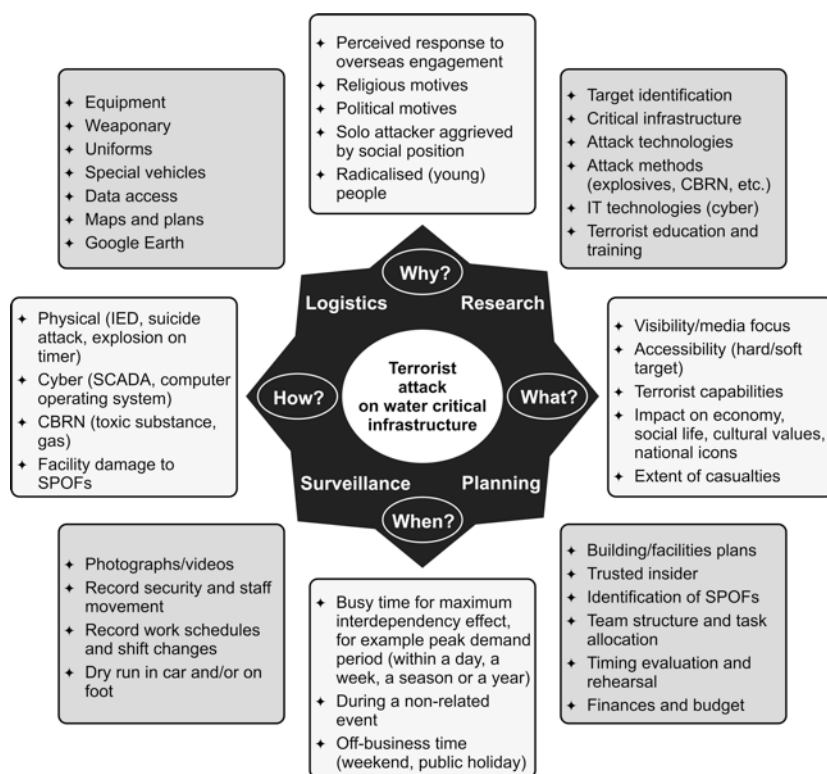


Figure 3: Potential terrorist attack targets in water critical infrastructure

4.2 Attack planning on water critical infrastructure

Assuming that water is a future terrorist target option, and that the areas of possible attack are also identified as in Figure 1, then consequently, it is potentially appropriate to examine the planning process that would occur, prior to any future attack. Figure 3, is a typical representation of the broad considerations faced by a terrorist group planning to attack water CI, with the described actions variable, relative to the size and composition of the group and the complexity of the planned attack. The planning process activities outlined in Figure 4 are complex, and often occur over a 3 month to 1 or more years (Bennett, 2007), and as indicated are extremely complex with a potential number of attacks considered simultaneously, to identify the highest profile attack, or for the terrorist group to maximise the injuries and deaths in some cases (Drake, 1998).



LEGEND: CBRN = chemical, biological, radiological, nuclear; IED = improvised explosive device; IT = information technology; SCADA = supervisory control and data acquisition; SPOF = single point of failure

Figure 4: Typical components of terrorist attack planning

However, Figure 4 illustrates the complexity and the range of alternative options available to the terrorist group when considering and planning attacks on water CI. Although there is no universal blueprint or exact model for terrorist attack planning strategies there are commonalities and strategies from other successful attacks that the various groups have learnt from, with the cross fertilization evident in personnel exchanges, training and information sharing between various cells and groups (Drake, 1998). Indeed as numerous studies indicate, water is a soft target and some attack planning has occurred internationally over the past 10 years (Kalil and Berns, 2004, Kroll et al., 2010a, Kroll, 2012b, Meinhardt, 2005, Meinhardt, 2006) related to water services.

During terrorist planning and addressing of the selection of the components required for a specific attack on water CI, there is some initial linkage and consideration as to the selection of the CI target relative to the ideology of the group, once a decision is confirmed to perform a terrorist attack. That is, what is the focus, and to a certain extent, what outcome is required. Typical of these are, significant media coverage, economic damage, and mass casualties, or even to prove themselves as a competent terrorist cell to their peers. (Bennett, 2007) describes three terrorist target measurement considerations as:

- The attractiveness of the target in regards to the attack accomplishing the terrorist's goals and objectives (which links to the ideology of the group).
- The potential threat level to the population with estimates of service disruption (for example water quality or supplies impacted across a wide area of society), facility and service damage with numbers of injuries and deaths amongst the selected population.
- Vulnerability, or 'softness', of the specific target, with indicative low levels of security to allow weapon



placement and adequate target access.

As some studies indicate, there is a pattern of planning and process adopted by all terrorists (Stewart, 2012, Drake, 1998) & (Lee, 2009a). Whether the 1970s models of left wing, such as the Red Brigades in Italy, the Irish Republican Army or the Baader-Mienhoff cell in Germany, or the more modern Islamic Fundamentalists such as al-Qaeda, al Shabaab, or Daesh, they all adopt and exhibit defined planning procedures and processes, with some commonalities (Lee, 2009a). A terrorist attack planning process, directed at water CI, would reflect some, or all of the pre-attack tasks, as indicated in Figure 5, dependent on the scale of the attack and the size of the terrorist group.

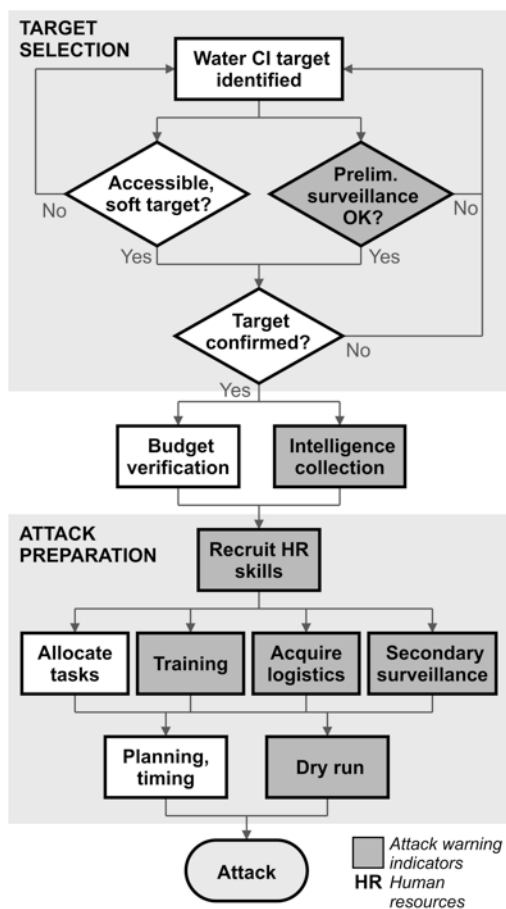


Figure 5: Terrorist attack planning process flowchart

4.3 Perceived threat levels on water critical infrastructure

International treated water critical infrastructure across continents and nations display many similarities. They all engage the functions of bulk water storage, filtration, and chemical treatment with water transport or distribution. Water CI is interlinked, with the growth of communities over time, and as such, often appear as illustrative 'spider webs' of distribution design meeting the cyclic and intermittent growth of cities, towns and communities. It is this form of system design, often spread geographically over large areas, which proves difficult to protect, and to ascertain the localised threat levels from deliberate adverse acts of human intervention, or terrorism. Assessment of the threat levels and vulnerability will change over time with considerations of various nation's population, economy coupled with national threat exposures to various



terrorist groups, and an understanding of terrorist motivations and their motivations to attack water CI (Haimés et al., 1998).

Furthermore, (Gleick, 1993) suggests that as time is progressing in the 21st century, water services are increasingly likely to be the targets of military or aggressive actions. Presently, there are considered to be “hundreds of threats against municipal water systems each year” in the United States (Beering, 2002). The potential for Terrorists to target and compromise water distribution systems is a widely recognised global CI vulnerability within the water industry by international researchers (Coleman, 2005, Court-Young, 2003, Kroll, 2009, Kroll, 2012a, Meinhardt, 2006). It is reported that recently, only a few terrorist threats have been directed against water supply systems, and those threats have not been widely publicised by the media (Haimés et al., 1998). However (Gleick and Heberger, 2014) document 108 individual attacks on water CI between 2000 and 2012. Furthermore, Gleick et al research sought examples and sources that were not always reported from media sources. It is feasible that the deficit of media reporting possibly creates a lax environment related to the water security perspective and activities of water CI owners. As (Gleick, 2006) further advises, “The chance that terrorists will strike at water systems is real but poorly understood by water managers and the public”.

Most business continuity and risk matrixes tend to accentuate the priorities for ‘high likelihood’ events, whereas any terrorist attack in most areas is considered ‘low likelihood’, but with high consequences related to the protection of life, property, the environment, with reputational considerations. As (Gilbert et al., 2003) highlights, the deliberate, adverse human asset intervention requires different levels of mitigation and protection, than for orderly historic process to mitigate natural or ‘all-hazard’ risks.

Many people in communities consider that water CI is not a target of terrorism for the reason that modern terrorist incidents appear to be interlinked with a form of ‘theatre’ (Kroll, 2006). Some researchers allude to an oblique association between the terrorist act and media amplification (Howie, 2009) providing the terrorist ‘oxygen’ for further future attacks. However, Kroll considers that an attack on water CI would potentially affect populations in a greater way than an airline attack or a transport terminal or restaurant, as a person can make a decision not to fly, or to avoid transport terminals or restaurants, but we all use and drink water (Kroll, 2006). Water CI is an essential service to all global populations and any potential future terrorist attacks will maximise disruption in communities, interrupting community development, striking emotion and fear across populations (Kroll, 2006).

Indeed, potable water systems are not the only potential target within water CI. Elevated exposures of risk exist in the further development of computer based water and wastewater control systems, such as SCADA (Byres et al., 2004, Hildick-Smith, 2005, Luijff et al., 2011). Furthermore, the wastewater sector of water CI exhibits some vulnerabilities, when the Guadalajara incident of 1992 is considered. In this incident, a massive explosion resulted in 252 people killed, nearly 500 injured and 15,000 left homeless. The estimated monetary damage ranges between \$300 million and \$1 billion, and 750 businesses failed to recover (EET, 1992) (Dugal, 1999). Although the Guadalajara incident was an accidental incident, it demonstrates the potential application of the wastewater system with adverse external human intervention, resulting in high casualties, economic and social disruption.

4.4 Discussion

The historical interpretation of water security prior to the modern phenomena of terrorism was water quality, pressure and supply availability. In the 21st century, it is more significantly, the physical and cyber security



of potable water and wastewater. It now requires the security assessment of the SPOFs along the water CI cycle in both systems. Typical of these are the storage, treatment facilities, transport and distribution with consideration of the security of service and product delivery to the consumer. There are significant new layers of security to be assessed, with each layer and component of water CI offering opportunities and challenges from bulk water storage to the end user. The objective is to harden water CI, to any potential future terrorist attack to inhibit the selection of water CI as a future target.

As water is perceived as essential to all life on the planet, some researchers consider that Islamic Jihadist extremists would be unlikely to plan and conduct an attack on water CI (Kroll, 2006). In contrast, (Kroll, 2006) indicates that interpretations from Islamic writings, such as “Those in the Garden will drink delicious wine, while those in the Fire will drink boiling water that will tear apart their intestines” (Kroll, 2006) (quoting Muhammad 47:15) may be construed to justify a future attack on water CI.

A converse view was expressed by Ronald Dick, former Deputy Head of the U.S. Federal Bureau of Investigation (FBI) in a 2001 testimony before the U.S. Congress. He stated that, “With regard to contamination by biological agents, the nation’s water supply may seem to be a logical target for a terrorist attack in reality, targeting the water supply may prove difficult. In order to be successful, a terrorist would have to have large amounts of agent and some knowledge of the water supply network and access to critical locations within the network ” (Dick, 2001, Kroll, 2006). Unfortunately, this statement occurred in 2001, and within that environment, law enforcement and risk managers were only considering bulk water storage as a potential target of concern.

However, in recent years and an escalated global terrorism environment, attitudes, opinions and assessments of water CI has progressed to consider that water CI is a target, and more significantly, the SCADA control systems and identified single points of failure across the CI system, downstream from the reservoirs and bulk water storages (Hildick-Smith, 2005). Indeed, (Copeland, 2010) advises that the in 2010, the U.S. Congress allocated USD\$923 Million to provide increased security at water CI and in particular, to assess and protect federal facilities and support security assessment and risk reduction activities by non-federal facilities and passed a bill requiring drinking water utilities to conduct security vulnerability assessments across water CI.

The U.S. government’s water CI target hardening may well reduce the likelihood of any future potential terrorist attack, as (Enders and Sandler, 1993) indicate, proactive policy measures and target hardening to ensure that potential terrorist attacks are more difficult, causes the terrorist to seek other targets that are ‘softer’ and easier to attack. This form of transference is well recognised and understood by researchers (Brandt, 2009), and when applied to the water CI this form of transference could well shift to water and its supply chain, as a form of impact on a current soft target to maximise the attack results required by the terrorist group.

The water CI sector is considered by (Porod et al., 2014) to represent a ‘lifeline’ sector to the majority of other CI. (Porod et al., 2014) further suggests “...it is essential to ensure both the protection and resilience of these systems in order for the successful treatment of water and wastewater to occur” (Porod et al., 2014). Accordingly, an assessment on the assets and supply chain related to criticality (how essential is the asset?) could be initiated by water CI owners. Considerations of these assessments are,

- **vulnerability** (How susceptible are the range of supply assets to surveillance and attack);
- **recoverability** (How difficult will it be to recover from inflicted damage, in consideration of time, special repair equipment, and manpower to restore the supply chain assets to normal functional



operation?).

- **current threat level**, and more importantly, how many water businesses regularly review the threat level from Terrorism? (Brown et al., 2005).

5 Conclusion

This paper reviewed two major areas of water and wastewater critical infrastructure (water CI), first, its dependencies including links to other critical infrastructures, and second, its security in relation to external adverse human interventions (i.e. terrorist attacks). Regarding security of water CI, the main focus is on attack planning considering its typical components and perceived threat levels on water CI as a 'soft' target.

The conclusions are summarised as follows. The lack of clear understanding by water sector managers of relevant dependencies and interdependencies can lead to an increase of water CI vulnerability, which could, in the case of an external attack, result in sudden and protracted failure. Development of future partnerships and linkages across the supply chains could increase awareness of potential failures, which could assist in reduction of potential impacts.

Water CI is recognized as a target. Hardening its protection is necessary in order to inhibit its selection as a subject of a terrorist attack. Security assessments would require identification of single points of failures (SPOFs) in both water and wastewater systems. Additionally, these assessments would require an evaluation of system vulnerability, recoverability and current threat level within specific nation social and political environments.

6 References

- AAP. 2003. Man Charged over Threat to Melbourne Water. *The Age*, January 31st 2003.
- ABC 2003. Man Who Threatened Melbourne Water Supply Bailed. Australian Broadcasting Network.
- ABRAMS, M. & WEISS, J. 2008. Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia. In: CORPORATION, T. M. (ed.). The MITRE Corporation, Springfield, VA, USA The MITRE Corporation & Applied Control Solutions.
- ALTMAN, P., CUNNINGHAM, J., DAHNESHA, U., BALLARD, M., THOMPSON, J. & MARSH, F. 2006. Disturbance of Cerebral Function in People Exposed to Drinking Water Contaminated With Aluminium Sulphate: Retrospective Study of the Camelford Water Incident. Oxford, UK: Oxford University, UK.
- BALMER, C. 2004. Italian Court Acquits Nine in Alleged Plot Against US Embassy. In: REUTERS (ed.). Reuters.
- BBC & ROSE, M. 2012. Camelford Water Poisoning: Authority 'Gambled With Lives'. URL: <http://www.bbc.co.uk/news/uk-england-cornwall-17367243> (Accessed on 12 December 2015). In: BBC (ed.).
- BEERING, P. S. 2002. Threats on Tap: Understanding the Terrorist Threat to Water. *Journal of Water Resources Planning and Management*, 128, 163-167.
- BENNETT, B. T. 2007. *Understanding, Assessing and Responding to Terrorism – Protecting Critical Infrastructure and Personnel*, New Jersey, USA, John Wiley & Sons.



- BIRKETT, D. & MALA-JETMAROVA, H. 2014. Plan, Prepare and Safeguard: Water Critical Infrastructure Protection in Australia. In: CLARK, R. M. & HAKIM, S. (eds.) *Securing Water and Wastewater Systems, Protecting Critical Infrastructure 2*. Switzerland: Springer International Publishing.
- BIRKETT, D., TRUSCOTT, J., MALA-JETMAROVA, H. & BARTON, A. F. 2011. Vulnerability of Water and Wastewater Infrastructure and its Protection from Acts of Terrorism: A Business Perspective. In: CLARK, R. M., HAKIM, S. & OSTFELD, A. (eds.) *Handbook of Water and Wastewater Systems Protection, Series Protecting Critical Infrastructure*. New York, USA: Springer.
- BOUWMANS, I., WEIJNEN, M. & GHEORGHE, A. 2006. Infrastructures at Risk. In: NETHERLANDS, S. (ed.) *Critical Infrastructures at Risk: Securing the European Electric Power System*. Netherlands: Springer.
- BRANDT, P. T. 2009. What do Transnational Terrorists Target? Has It Changed? Are We Safer? California: US Department of Homeland Security (DHS), Center for Risk and Economic Analysis of Terrorism Events (CREATE).
- BROCKETT, J. 2015. UK Water Networks Vulnerable to Terrorist Attack. In: [HTTP://UTILITYWEEK.CO.UK/NEWS/UK-WATER-NETWORKS-%E2%80%98VULNERABLE-TO-TERRORIST-ATTACK/1150512#.VKC-C8TOCYU](http://UTILITYWEEK.CO.UK/NEWS/UK-WATER-NETWORKS-%E2%80%98VULNERABLE-TO-TERRORIST-ATTACK/1150512#.VKC-C8TOCYU), O.-L. U. W. U. (ed.). Utilities Week.
- BROWN, G., CARLYLE, M., SALMERON, J. & WOOD, K. 2005. Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses. *INFORMS Tutorials in Operations Research*. Institute for Operations Research and the Management Sciences, Hanover, MD.
- BROWN, T., BEYELER, W. & BARTON, D. 2004. Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for Complex Adaptive Systems. *International Journal of Critical Infrastructures*, 1, 108-117.
- BYRES, E. J., FRANZ, M. & MILLER, D. 2004. The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. *International Infrastructure Survivability Workshop (IISW'04), IEEE*. Lisbon, Portugal, 5-8 December 2004.
- CAMERON, C. 2002. Feds Arrest al-Qaeda Suspects with Plans to Poison Water Supplies. In: NEWS, F. (ed.). Fox Media. URL: <http://www.foxnews.com/story/2002/07/30/feds-arrest-al-qaeda-suspects-with-plans-to-poison-water-supplies/>.
- COHEN, F. 2010. What Makes Critical Infrastructures Critical? *International Journal of Critical Infrastructure Protection, Elsevier*, 3, 53-54.
- COLEMAN, K. 2005. Protecting the Water Supply From Terrorism. In: [HTTP://WWW.DIRECTIONS.MAG.COM/ENTRY/PROTECTING-THE-WATER-SUPPLY-FROM-TERRORISM/123563](http://WWW.DIRECTIONS.MAG.COM/ENTRY/PROTECTING-THE-WATER-SUPPLY-FROM-TERRORISM/123563), D. M. O.-L. U. (ed.). United States of America: Directions On-Line Magazine.
- COLES, I. 2014. Iraq Insurgents Use Water as a Weapon After Seizing Dam. Reuters. URL: <http://www.reuters.com/article/2014/04/11/us-iraq-security-idUSBREA3A0Q020140411>.
- COOK, C. & BAKKER, K. 2012. Water Security: Debating an Emerging Paradigm. *Global Environmental Change*, 22, 94-102.
- COOPER, A. 2013. Man's al-Qaeda Link. *The Melbourne Age, Australia*. URL: , Tuesday April 09, 2013.
- COPELAND, C. 2010. Terrorism and Security Issues Facing the Water Infrastructure Sector. Washington, U.S.A.: CRS Report for Congress, Congressional Research Service.



- COPELAND, C. & CODY, B. 2003. Terrorism & Security Issues Facing the Water Infrastructure Sector. *In: CONGRESS, U. S. (ed.)*. Washington, DC, U.S.A.: U.S. Congress.
- COURT-YOUNG, H., C. 2003. *Understanding Water and Terrorism*, Denver, Colorado, U.S.A., Burg Young Publishing LLC.
- COVERT, A., J. 2008. *Water: Vital to Life, Vulnerable to Terrorism*. PhD Partial Fulfillment of the Graduation Requirements, Air University. Maxwell Air Force Base, Alabama, USA.
- CRC 2008. Drinking Water Treatment. *In: TREATMENT, T. C. R. C. F. W. Q. A. (ed.) Drinking Water Facts*. Issue 2 ed. Adelaide, South Australia: The Cooperative Research Centre for Water Quality and Treatment.
- DICK, R. L. 2001. Terrorism: Are America's Water Resources and Environment at Risk? *Subcommittee on Water Resources and Environment*. Washington, DC, USA: House Committee on Transport and Infrastructure.
- DRAKE, C. J. M. 1998. *Terrorists' Target Selection*, London, U.K., MacMillan Press.
- DREAZEN, Y., J. 2001. Officials Fear Terrorists Could Use 'Backflow' To Put Toxins Into Water Distribution Grids. *The Wall Street Journal*, 27th December 2001, p.1.
- DUGAL, J. 1999. Guadalajara Gas Explosion Disaster. *Disaster Recovery Journal*, 5, http://www.drj.com/drworld/content/w2_028.htm (Accessed on 21 January 2012).
- E.P.A. 2000. The History of Water Treatment. *In: AGENCY, E. P. (ed.)*. Washington, United States of America: Environmental Protection Agency- Office of Water.
- EET 1992. 1992 Guadalajara explosions. U.S.A. http://everything.explained.today/1992_Guadalajara_explosions/ (Accessed on 02 December 2015).
- ENDERS, W. & SANDLER, T. 1993. The Effectiveness of Anti-Terrorism Policies: A Vector-Autoregression-Intervention Analysis. *American Political Science Review*, 87, 829-844.
- FEUER, A. 2003. Jordan Arrests Iraqis in Plot to Poison U.S. Troops' Water. *New York Times*. URL: <http://www.nytimes.com/2003/04/01/international/worldspecial/01CND-JORD.html>.
- GILBERT, P. H., ISENBERG, J., BAECHER, G. B., PAPAY, L. T., SPIELVOGEL, L. G., WOODARD, J. B. & BADOLATO, E. V. 2003. Infrastructure Issues for Cities—Countering Terrorist Threat. *Journal of Infrastructure Systems*, 9, 44-54.
- GILLETTE, J., FISHER, R., PEERENBOOM, J. & WHITFIELD, R. 2002. Analysing Water/Wastewater Infrastructure Interdependencies *6th International Conference on Probabilistic Safety Assessment and Management (PSAM6)*. San Juan, Puerto Rico, USA, 23-28 June 2002.
- GLEICK, P. H. 1993. Water and Conflict: Fresh Water Resources and International Security. *International Security*, 18, 79-112.
- GLEICK, P. H. 1996. Basic Water Requirements for Human Activities: Meeting Basic Needs. *Water international*, 21, 83-92.
- GLEICK, P. H. 2006. Water and Terrorism. *Water Policy*, Volume 8, 481-503.
- GLEICK, P. H. & HEBERGER, M. 2014. Water Conflict Chronology. *The World's Water, Volume 8*. California, USA: Pacific Institute.



- HAIMES, Y. Y., MATALAS, N. C., LAMBERT, J. H., JACKSON, B. A. & FELLOWS, J. F. R. 1998. Reducing Vulnerability of Water Supply Systems to Attack. *Journal of Infrastructure Systems*, 4, 164-177.
- HICKMAN, D. C. 1999. A Chemical and Biological Warfare Threat: USAF Water Systems at Risk. Alabama, <http://www.au.af.mil/au/awc/awcgate/cpc-pubs/hickman.pdf> (Retrieved 19 January 2012): USAF Counterproliferation Center, Maxwell Air Force Base.
- HILDICK-SMITH, A. 2005. Security for Critical Infrastructure Scada Systems. SANS Reading Room, SANS Institute, Bethesda, Maryland: GSEC Practical Assignment, Version 1.4c, 23 February 2005.
- HOKSTAD, P., UTNE, B. I. & VATN, J. 2012. *Risk & Interdependencies in Critical Infrastructures—A Guideline for Analysis*, Springer—London, Heidelberg, New York, Dordrecht, Springer.
- HOWIE, L. (ed.) 2009. *Terrorism, the Worker and the City—Simulations and Security in a Time of Terror*, Farnham, UK: Gower.
- IRELAND, E. 2011. Water Treatment Manual—Disinfection. Wexford, Ireland. URL: http://www.epa.ie/pubs/advice/drinkingwater/disinfection2_web.pdf: EPA.
- KALIL, J. M. & BERNS, D. 2004. Drinking Supply: Terrorist Had Eyes on Water. In: JOURNAL, R. (ed.). Washington U.S.A. URL: <http://www.defendyourh2o.com/pdfs/DRINKING%20SUPPLY.pdf>.
- KHAN, S. & HANJRA, M. A. 2009. Footprints of Water and Energy Inputs in Food Production—Global Perspectives. *Food Policy*, 34, 130-140.
- KROLL, D. 2006. *Securing Our Water Supply: Protecting a Vulnerable Resource*, Tulsa, Oklahoma, United States of America. , PennWell Corporation.
- KROLL, D. Testing the Waters: Improving Water Quality and Security Via On-Line Monitoring. ICMA, 22nd September 2008 2008 Richmond VA, U.S.A. URL: http://hachhst.com/wp-content/uploads/2010/07/Presentation_Water-Security-and-Quality.pdf (Accessed 04.12.2015). Richmond VA, U.S.A., 89 Pages.
- KROLL, D. 2010. Aqua ut a Telum “Water as a Weapon”. Colorado, United States of America. URL: http://hachhst.com/wp-content/uploads/2010/07/White-Paper_Water-as-a-weapon.pdf (Accessed 24.11.2015): Hach Homeland Security Technologies.
- KROLL, D., J 2012a. The Terrorist Threat to Water and Technology’s Role in Safeguarding Supplies. 16.
- KROLL, D., J. 2009. Water Distribution Monitoring: Opportunities and Challenges for Enhancing Water Quality and Security. In: TECHNOLOGIES, H. H. S. (ed.). Colorado, U.S.A.: Hach Homeland Security Technologies.
- KROLL, D., J. 2012b. The Terrorist Threat to Water and Technology’s Role in Safe Guarding Supplies. USA.
- KROLL, D., J., KING, K., ENGELHARDT, T., GIBSON, M., CRAIG, K. & SECURITIES, H. H. 2010a. Terrorism Vulnerabilities to the Water Supply and the Role of the Consumer: A Water Security White Paper. Water World On -Line Journal.
- KROLL, D., KING, K., ENGELHARDT, T., GIBSON, M. & CRAIG, K. 2010b. Terrorism Vulnerabilities to the Water Supply and The Role of the Consumer: A Water Supply White Paper. In: TECHNOLOGIES, H. H. (ed.). Waterworld.
- LAZAROVA, D. 2015. Problem With Contaminated Tap Water in Prague 6 Still Unresolved. In: PRAHA, R. (ed.). Radio Praha. URL: <http://www.radio.cz/en/section/news/problem-with-contaminated-tap-water-in-prague-6-still-unresolved> (Date accessed 27.05.2015).



- LEE, E. 2009a. *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection*, Boca Rato, Florida, U.S.A., Auerbach Publications.
- LEE, J.-J. M. 2009b. A War for Water. *World Environmental and Water Resources Congress 2009: Great Rivers*. Kansas City, Missouri: American Society of Civil Engineers.
- LUIJF, E., ALIB, M. & ZIELSTRAB, A. 2011. Assessing and Improving SCADA Security in the Dutch Drinking Water Sector. *International Journal of Critical Infrastructure Protection, Elsevier*, 4, 124-134.
- MEINHARDT, P., L. 2005. Water and Bioterrorism: Preparing for the Potential Threat to U.S. Water Supplies and Public Health. *Annual Review of Public Health*, 24, 213-237.
- MEINHARDT, P., L. 2006. Medical Preparedness for Acts of Water Terrorism. In: MEDICINE, A. C. O. P. (ed.). U.S.A.: American College of Preventative Medicine.
- MONITOR, P. D. 2015a. Prague to Vaccinate Children From Districts With Contaminated Water. URL: <http://praguemonitor.com/2015/06/08/prague-vaccinate-children-districts-contaminated-water> (Accessed on 08 June 2015).
- MONITOR, P. D. 2015b. Prague Town Hall Files Complaint Over Contaminated Drinking Water.: URL: <http://www.praguemonitor.com/2015/05/28/prague-town-hall-files-complaint-over-contaminated-drinking-water> (Accessed on 26 November 2015).
- MORRIS, S. 2012. The Camelford Poisoning: Blackwater, A Driver's Mistake.
- NOBLE, T. & SCHREMBI, J. 1984. Geelong Man Charged over Poisoning Threat. *The Melbourne Age*, 17th September 1984, p. Page 1.
- PALANIAPPAN, M., GLEICK, P. H., ALLEN, L., COHEN, M., J., CHRISTIAN-SMITH, J. & SMITH, C. 2010. Clearing the Waters: A Focus on Water Quality Solutions. In: ROSS, N. (ed.). Nairobi, Kenya, Africa: Pacific Institute.
- PIMENTEL, D., HOUSER, J., PREISS, E., WHITE, O., FANG, H., MESNICK, L., BARSKY, T., TARICHE, S., SCHRECK, J. & ALPERT, S. 1997. Water Resources: Agriculture, the Environment, and Society. *BioScience*, 97-106.
- POROD, C., COLLINS, M. & PETIT, F. 2014. Water Treatment Dependencies. *The CIP Report*. URL: <http://cip.gmu.edu> (Accessed on 10 April .2015), Volume 13, 10-13.
- RANSTORP, M. (ed.) 2007. *Mapping Terrorism Research*, Abingdon: Routledge.
- REID, S. 2007. Camelford A Lethal Cover Up: Britain's Worst Water poisoning Scandal. In: MAIL., D. (ed.). Daily Mail. URL: <http://www.dailymail.co.uk/news/article-502442/A-lethal-cover-Britains-worst-water-poisoning-scandal.html> (Accessed on 03 December 2015).
- RINALDI, S. M. 2004. Modeling and Simulating Critical Infrastructures and Their Interdependencies. *37th Hawaii International Conference on System Sciences*. Big Island, Hawaii, 5-8 January 2004: IEEE.
- SCHUTTE, E. 2006. Handbook for the Operation of Water Treatment Works. Department of Chemical Engineering, University of Pretoria, South Africa, : Water Institute of South Africa, Water Research Commission (WRC).
- SILVA, C. J. 2011. Attempted Water Poisoning in Spain. Gates of Vienna. URL: <http://gatesofvienna.blogspot.cz/2011/08/more-on-attempted-water-poisoning-in.htm> (Accessed on 16 June 2015).



SNOW, J. 1857. Cholera, and the Water Supply in the South Districts of London. *British Medical Journal*, 4, 864-865.

STEWART, S. 2012. Detection Points in the Terrorism Attack Cycle. *Security Weekly: Fundamentals of Terrorism*, Chapters 3 and 5.

SULLIVAN, J., K. 2011. Water Sector Interdependencies–Summary Report. Alexandria, VA, USA: Water Environment Federation.

TURCIOS, R. M., WIDDOWSON, M.-A., SULKA, A. C., MEAD, P. S. & GLASS, R. I. 2006. Re-evaluation of Epidemiological Criteria for Identifying Outbreaks of Acute Gastroenteritis Due to Norovirus: United States, 1998–2000. *Clinical Infectious Diseases*, Volume 42., Issue 7., 964-969.

WEISS, J. 2011. Hackers ‘Hit’ US Water Treatment Systems. *BBC News Technology*. URL: <http://www.bbc.co.uk/news/technology-15817335> (Accessed on 28 January 2012), 21 November 2011, p.1.

WILLOUGHBY, I. 2015. Anger after slow announcement of water contamination leaves scores sick in Prague. URL: <http://www.radio.cz/en/section/curraffrs/anger-after-slow-announcement-of-water-contamination-leaves-scores-sick-in-prague> (Accessed 27.07.2015). Radio Praha. CZ. .

WOLF, A. T. 2007. Shared Waters: Conflict and Cooperation. *Annual Review of Environment and Resources*, 32, 3.1-3.29.

WOLF, A. T., KRAMER, A., CARIUS, A. & DABELKO, G. D. 2005. Managing water conflict and cooperation. *State of the World 2005: Redefining Global Security*. . The World Watch Institute.

Notes

[1] GLEICK, P. H. 1993. Water and Conflict: Fresh Water Resources and International Security. *International Security*, 18, 79-112. Pp 79.

[2] SPOFs = Single Points of Failure

About the author: David Birkett is based in the Czech Republic with Truscott Crisis Leaders (Australia). Dave has worked across the three tiers of government, and in the public and private sector in the water, power, mining, oil, gas and transport industries. He has specialised in the risk and emergency management, disaster mitigation planning and business continuity, with the emergency response aspects of managing public and private sector assets. Dave has applied his expertise with counter intelligence in Defence, Australia to advise organisations in the prevention and control of emergencies and crises. Dave’s developed expertise is in the design and delivery of training in emergency response, and crisis management to middle and senior managers in the oil & gas, power, utilities, chemical and other high risk industries. Experienced in leading and coaching crisis and emergency management teams in their roles and responsibilities during major emergencies. Other activities include competency assessments, delivering training in the form of presentations on various subjects involved in Crisis and Emergency Response, such as, HR, communications, command and control, information handling, emergency control centre dynamics, roles & responsibilities, logistic and resource allocation, Dave is currently progressing study towards his PhD as an independent Researcher in the field of critical infrastructure protection. Specialties: • Risk, emergency and crisis management • Prevention and control of emergencies and crises • Disaster mitigation planning including crisis simulation exercises (CSE) • Business continuity • Security investigations • Leading of project teams • Implementing processes and physical change Protective strategies for



The Centre for the Study of Terrorism and Political Violence

Journal of Terrorism Research



Critical Infrastructure protection.