THE TERROR RISK TO CURRENT WATER INFRASTRUCTURE SYSTEMS

BY GIOVANNA CIOFFI

SUBMITTED 9 FEBRUARY 2015

A MAJOR PAPER IS SUBMITTED TO
THE FACULTY OF ENVIRONMENTAL STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER IN ENVIRONMENTAL STUDIES

YORK UNIVERSITY
TORONTO, ONTARIO, CANADA

GIOVANNA CIOFFI, MES CANDIDATE **L. ANDERS SANDBERG, SUPERVISOR**

ABSTRACT

Unquestionably, water maintains a critical role within society. It is precisely this role that makes it an attractive target for potential adversaries. As it currently stands, water infrastructures are significantly vulnerable to attacks; their risk however, is questionable. As such, this work will analyze the security of water infrastructure systems. It will discuss the systems involved in the treatment of water and waste water, and how various processes can be vulnerable to four main threats: biological, chemical, cyber and physical threats. Additionally, this work will challenge the conventional view of terrorism through the perspective of Critical Terrorism Studies as a means to discuss how non-traditional threats such as privatization and neoliberalization may also be seen as threats. Moreover, this work will also explore how each of these threats may be realized, and it will furthermore utilize case studies and professional interviews to achieve this.

Attacks upon water infrastructure systems are not new. In fact, such attacks have been reported as far back as 500 BCE. What is new, however, is the evolving threat landscape. Given the convenience of the Internet, a single individual can research almost any topic to his or her desire, including vulnerabilities within critical infrastructure systems. To add to this, one does not have to search deep into the web to find information on how to inflict serious damage. Certainly, the twenty-first century has its prospects, but it certainly has its perils as well. This work will attempt to address vulnerabilities, and furthermore, what is at stake if nothing remains to be done.

FOREWORD

This Major Paper fulfills the requirements of the Master of Environmental Studies degree by incorporating components of my area of concentration of dangerous technology, terrorism, and disaster management with a view to analyze the vulnerabilities of modern water infrastructure. Proficiency on this topic requires an understanding of current and alternate water infrastructure systems, in addition to their threat sources.

The nature and role of this major paper is to shed light on the potential threats to water infrastructure systems in Toronto, Ontario. This work aims to look deeper into a subject that is not publically spoken about, given its sensitive nature. In doing so, it is the hope of the author that it dispenses information that provides the reader with a greater sensitivity to the traditional and non-traditional threats present within their environment. Although the author offers her own assessment in the conclusion of this work, it is hoped that this work will also encourage one to draw their own assessment and contribute to the security of the water infrastructure.

Although the objectives for each of the components were predominantly completed through coursework and certifications, this Major Paper provided the circumstances to explore the topic of terrorism through the two perspectives: conventional and critical terrorism studies, and finally, to relate these two perspectives back to the three components of the plan of study.

Two of the components, dangerous technology and terrorism, are addressed by analyzing conventional and critical terrorism studies. Later on in this work, they are also addressed by analyzing the physical, cyber, chemical and biological threats that exist within the current water infrastructure systems.

The third component of disaster management is addressed through the lens of critical infrastructure protection. Illustrating the systems and identifying the vulnerabilities, and moreover analyzing case studies has provided the insight necessary to understand the vulnerabilities that currently exist. It has also provided the foundation of understanding why water infrastructure is a target of interest to potential adversaries.

ACKNOWLEDGEMENTS

MANY THANKS TO MY INITIAL ADVISOR AND SUPERVISOR, S.H. ALI, FOR HIS ADVICE AND GUIDANCE THROUGH THE INTIAL STAGES OF THIS PROGRAM. I WOULD ALSO LIKE TO THANK L.A. SANDBERG WHO CONTINUED TO PROVIDE THE GUIDANCE AND SUPPORT NECESSARY TO COMPLETE THIS MAJOR PAPER. YOUR TIME AND EFFORT ARE GREATLY APPRECIATED.

TO EACH OF THE PARTICIPANTS WHO DISPENSED THEIR KNOWLEDGE

TO EVERYONE WHO REMINDED ME THAT THE ONLY REWARD IN TAKING THE EASY WAY OUT, IS THAT IT'S EASY

TO CNJB, DK, WJP FOR YOUR ENDLESS FAITH, LOVE, SUPPORT AND LOYALTY

TO MY FRIENDS AND FAMILY

FOR EVERYONE WHO WILL CONTINUE TO BE PRESENT THROUGHOUT THIS FIGHT

THANK YOU.

TABLE ON CONTENTS

LIST OF FIGURES AND TABLES

FIGURES

TABLES

GLOSSARY OF TERMS

ACTUS REUS: "The act or omissions that comprise the physical elements of a crime as required by statute" (Cornell, 2014, 1).

AVAILABILITY: "Assets can be accessed or used by authorized parties as needed" (Conklin, 2011, 77).

CONFIDENTIALITY: "Relates to keeping secrets about assets secret" (Conklin, 2011, 77).

CRITICAL INFRASTRUCTURE: "Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence" (PSC, 2014, 1).

INTEGRITY: "Focuses on preventing unauthorized changes to assets" (Conklin, 2011, 77).

INTERNET OF THINGS: "The Internet of Things represents an evolution in which objects are capable of interacting with other objects. Hospitals can monitor and regulate pacemakers long distance, factories can automatically address production line issues and hotels can adjust temperature and lighting according to a guest's preferences, to name just a few examples. Furthermore, as the number of devices connected to the Internet continues to grow exponentially, your organization's ability to send, receive, gather, analyze and respond to events from any connected device increases as well" (IBM, 2014).

MENS REA: "The psychological state defining a criminal perpetrator as culpable for having committed a crime" (Cornell, 2014, 1).

MITIGATION: "Actions taken to reduce the adverse impacts of an emergency or disaster. Such actions may include diversion or containment measures to lessen the impacts of a flood or a spill" (EMO Glossary of Terms, 2011).

MULTI-PARAMETER MONITORING: "Multi-parameter monitoring entails monitoring common water quality parameters and then looking for anomalies that may be indicative of a water contamination event. Sensors can include parameters such as chlorine residual, total organic carbon, pH, conductivity, turbidity, UV absorbance/fluorescence and others" (Kroll, 2013, 12).

PREPAREDNESS: "Actions taken prior to an emergency or disaster to ensure an effective response. These actions include the formulation of emergency response plans, business continuity/continuity of operations plans, training, exercises, and public awareness and education" (EMO Glossary of Terms, 2011).

PREVENTION: "Actions taken to stop an emergency or disaster from occurring. Such actions may include legislative controls, zoning restrictions, improved operating standards/procedures or critical infrastructure management" (EMO Glossary of Terms, 2011).

RECOVERY: "The process of restoring a stricken community to a pre-disaster level of functioning. This may include the provision of financial assistance, repairing buildings and/or restoration of the environment" (EMO Glossary of Terms, 2011).

RESPONSE: "The provision of emergency services and public assistance or intervention during or immediately after an incident in order to protect people, property, the environment, the economy and/or services. This may include the provision of resources such as personnel, services and/or equipment" (EMO Glossary of Terms, 2011).

RISK: "The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. Threat x Probability x Business Impact = Risk" (Maniscalchi, 2009, 1).

SCADA AND DCS: "There are two primary types of control systems: Distributed Control Systems (DCS), which are typically used within a single processing or generating plant, or over a small geographic area; and Supervisory Control and Data Acquisition (SCADA) systems, which are used for large, geographically dispersed distribution operations. As an example, a utilities company may use a DCS to generate power and a SCADA system to distribute it" (Gendron and Rudner, 2012, 49-50).

TERRORISM: "A synthesis of war and theatre, a dramatization of the most proscribed kind of violence- that which is deliberately perpetrated on civilian non-combatant victims – played before an audience in the hope of creating a mood of fear, for political purposes" (Combs, 2011, 5).

TOXICITY MONITORING: "Toxicity tests are an attempt to measure toxicity in a sample by analyzing the results that exposure produces on standard test organisms" (Kroll, 2013, 11).

VULNERABILITY: "The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved" (Maniscalchi, 2009, 1).

WATER- AS-TARGET FOR ATTACK: "Water supplies can be poisoned; dams can be destroyed to harm downstream population " (Gleick, 2006, 4-5).

WATER-AS-TOOL FOR ATTACK: "Water resources or systems can be used as delivery vehicles to cause violence to a human population" (Gleick, 2006, 4).

CHAPTER 1 INTRODUCTION

1.1. PERSPECTIVES

This work is intended to be an identification and analysis of the vulnerabilities within water infrastructure systems. I do not intend it to be based on a discourse of fear, uncertainty and doubt. Instead, its purpose is to create awareness and prompt further mitigation strategies that will increase the resilience of this infrastructure.

Thus far in the twenty-first century it is adamantly clear that no technology can evade risk. Although it may certainly aid in one's knowledge of the threat spectrum, there can be no doubt that significant challenges lay ahead. This is true not only for "natural" disasters which appear to be increasing in strength and duration, but also for human-made technological disasters as a result of how modern cities, like Toronto, are interconnected and interdependent upon an array of assets and platforms. The *Internet of Things*[1] is one phrase that seeks to describe this increasing relationship of interconnectivity among platforms that have previously never been linked together.

When one conceives of the notion of water security, one often thinks of climate change, pollution and universal access to clean water. The threat of terrorism is a narrative that is not often included as part of this discourse. Professionals in domestic and international security are more often likely to explore this subject.

On this note, it is of value to indicate that the author is approaching this work with a background in emergency management and international security studies. Specifically, the author's previous studies focused on securing the electric grid's industrial control systems from cyber attacks. For the author, work in this field has provided a foundation for how

[1] The Internet of Things refers to: "The Internet of Things represents an evolution in which objects are capable of interacting with other objects" (IBM, 2014). Please refer to glossary of terms for further detail.

security is understood through factors such as confidentiality[2], integrity[3] and availability[4]. Together, these factors are central to critical infrastructure protection and, furthermore, in maintaining public confidence.

As such, the author is writing from the perspective that initiating proactive measures in opposition to relying on reactive response is necessary to ensure the safety and security of critical infrastructure. This is best illustrated in the five pillars of emergency management set out by Emergency Management Ontario. These five pillars consist of prevention, mitigation, preparedness, response and recovery (EMO, 2009).

It is the objective of this work to collect information that identifies the vulnerabilities within water infrastructure systems, and from here to analyze the current level of risk from the perspective of two narratives: a conventional terrorism and critical terrorism studies perspective. The former is the one with which the author is most familiar and it is based on the assumption that the potential for terrorism emanating from external threats, individual or organized, is real and that precautionary measures and planning need to be invoked to meet that threat. The latter perspective challenges the author to think about terrorism in broader terms and in the context of other threats to water infrastructure, including the dangers associated with poor maintenance, lack of funding, and the reluctance to develop alternative technologies.

In Chapter 2, I identify the importance of protecting water supplies and outlining the two perspectives on terrorism studies. In Chapter 3, I describe the dominant water infrastructure system and its nature and functions. In Chapter 4, I investigate the potential

[2] Please refer to the glossary of terms for definition of these terms.

[3, 4] Please refer to the glossary of terms for definition of these terms.

terrorist threats through the conventional lens of terrorism studies, using academic literature, case studies, and interviews of people in the industry. Finally, in Chapter 5, I utilize the case study on Walkerton to analyze the critical terrorism studies perspective on water security, in addition to briefly discussing sustainable water management and low-impact development. Chapter 6 will present the author's assessment, and the appendices provide additional information cited throughout this work.

CHAPTER 2 THE IMPORTANCE OF PROTECTING WATER SUPPLIES FROM TERRORISM: TWO PERSPECTIVES

No living organism is self-sustaining. Although the means of survival has changed drastically over the years - especially for humans - nothing changes the fact that humans need water to survive. As time has passed, technology has allegedly improved, and so has, at least for some, standards of living. For most Canadians, instead of fetching water, it now conveniently pours out of the taps in their homes.

Modern societies are built within and around networks of infrastructures that allow it to function. Generally, these infrastructures are often referred to as *critical infrastructure*, and include any necessary societal functions such as power generation, transmission and distribution, the continuity of government, communication networks, transportation networks, and among various others, water supply, treatment, storage and distribution networks. The reality of the twenty-first century is that modern societies are inherently dependent, interdependent and interconnected to each of these critical infrastructure systems.

Every day, Toronto treats more than one billion litres of potable water (City of Toronto, 2014). Each day, people are *dependent* on the City, not only to provide them with this invaluable resource, but to also ensure that it is safe to consume. The significance of ensuring a municipality's water infrastructure is safe rests on different levels of government.

2.1. WATER AS A TOOL VS. TARGET

History is rampant with "terrorist" attacks on water supplies. There has been no shortage of creativity either. From the Assyrians poisoning enemy wells before 500 BCE (Frischknecht, 2008, 2), to evidence of Al Qaeda's "interest in using cyanide, *Botulinum toxin* (Botox), *Salmonella typhi* (the causative agent of typhoid fever), and *Bacillus anthracis* (the causative agent of Anthrax) to attack US water systems" (Van Leuven, 2011, 35). There are plenty of examples where water has been utilized as both a tool and a target for attack. It is understood that utilizing water as a tool for an attack occurs when water supplies are used as delivery vehicles to carry a destructive agent to the targeted human population. In comparison to this, utilizing water as a target occurs when the resource itself is targeted for destruction or at least jeopardization, and the collateral damage is felt by the targeted population (Chalecki, 2001, 52).

YEAR	EVENT	DISEASE AGENTS AND OUTCOMES
< 500 BCE	▪ ASSYRIANS POISONED ENEMY WELLS	▪ RYE ERGOT FUNGUS CAUSING HALLUCINATIONS
590 BCE	▪ GREEKS POISON WATER SUPPLY OF KIRRHA DURING FIRST SACRED WAR	▪ HELLEBORE ROOT CAUSING DIARRHEA. KIRRHA FALLS AND THE POPULATION IS SLAUGHTERED
1346	▪ TARTARS CATAPULT PLAGUE VICTIMS OVER THE WALLS OF CAFFA	▪ YERSINIA PESTIS (PLAGUE) CAUSING PLAGUE. CITY IS ABANDONED

TABLE 1: SELECTION OF POSSIBLE EVENTS OF BIOLOGICAL WARFARE
SOURCE: MODIFIED FROM (FRISCHKNECHT, 2008, 2). FOR ADDITIONAL EXAMPLES, PLEASE REFER TO APPENDIX 1.

Society's dependence on water resources makes it an ideal and attractive target of opportunity. As it currently stands, the Canadian government recognizes the water sector as a critical infrastructure and, as a result, it is protected under Public Safety Canada

provisions (PSC, 2014). Despite this, the federal government's participation in the safekeeping of the water sector is rather limited. This is because the main responsibility for securing the water sector is maintained by the provincial government, and the municipal suppliers. In this regard, it is necessary to understand the vulnerabilities of the systems and networks at hand, and moreover, determine if there is a credible risk to Canada's water infrastructure.

2.2. Defining Threats, Security and Terrorism From a Conventional Terrorism Studies Perspective

One dictionary definition of a threat is "an expression of intention to inflict evil, injury, or damage" (Merriam-Webster, 2014). It corresponds well with how terrorism is understood from a conventional point of view. In particular, a threat may be a reactive or proactive approach for the purposes of garnering attention, to intimidate or terrorize an audience, or, for the purposes of coercion. Threat is typically associated with security. The United States Department of Homeland Security, defines security as "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters" (DHS, 2014). Examples of security measures may include fences, screen locks, antivirus software (DHS, 2014), identification pass cards, and closed-circuit television to name a few. Considered together, threats (past, present and future) propel the need for security measures to be in place.

Conceivably a much more complex term, terrorism is not as easily defined. Historically, the meaning of terrorism has changed drastically since its records of the Assassins in the eleventh century, to the Regimé de la Terreur in the eighteenth century, and even to more recent activities of terrorist-labeled groups such as the Environment

Liberation Front (ELF), Al Qaeda, the Islamic State of Iraq and Syria (ISIS) and the Liberation Tigers of Tamil Eelam (PSC, 2014b). It is important to note here that there is no internationally agreed definition of what constitutes terrorism[5]. Although there are a number of reasons for this definitional impasse, the main issue emanates from the decision to define terrorism to "exclude armed struggle for liberation and self-determination"[6] (Human Rights Voices, 2014).

Even without a legal definition, terrorism has been categorized into different *types* according to its motivation. For example, it is not strange for the media to use terms such as *environmental* terrorism, *eco*-terrorism, *religious* terrorism, or *political* terrorism when various agencies report on such events. Although these terms have virtually become mainstream, it is important to consider this contentious issue from a number of perspectives.

According to Bruno Frey, any attempt to define terrorism often results in two types of error almost instantaneously: "(1) activities that should reasonably count as terrorist acts are excluded and (2) activities that are not terrorist acts are included…one specific definition will essentially miss the goal of clarifying the issue, and will instead lead to confusion" (Frey, 2004, 9). In addition to this, there are a number of dependents to consider in the attempt to define terrorism.

As stated by Grant Wardlaw, one of these dependents includes justification (1990). Since justification is dependent on the interpretation of morals, Wardlaw argues that

[5] Where this work does mention terrorism, it defines it as follows: "A synthesis of war and theatre, a dramatization of the most proscribed kind of violence- that which is deliberately perpetrated on civilian non-combatant victims –played before an audience in the hope of creating a mood of fear, for political purposes" (Combs, 2011, 5).

[6] "This claim purports to exclude blowing up certain civilians from the reach of international law and organizations. It is central to interpreting every proclamation by the states which have ratified these conventions in any UN forum purporting to combat terrorism" (Human Rights Voices, 2014).

terrorism can be regarded as a moral problem where some cases of violence are justifiable and others are not (Wardlaw, 1990, 4). For example:

> The Palestine Liberation Organization [PLO] is seen by some nations as a terrorist group having no political legitimacy and using morally unjustifiable methods of violence to achieve unacceptable ends. On the other hand, other nations view the PLO as the legitimate representatives of an oppressed people using necessary and justifiable violence [not terrorism] to achieve just and inevitable ends. The definition rests, then, on moral justification (Wardlaw, 1990, 4-5).

This example further insinuates the notion that *one person's terrorist is another person's freedom fighter*. Essentially, moral justification is contained within the individual – in their beliefs and experiences. Similar to this, the justification of terrorism is also rooted in the social meaning that is assigned to the word terrorism (Wardlaw, 1990, 5), thereby asserting that one individual's definition of terrorism may not be in line with another individual's analysis, just as one's interpretation of justice may differ from other interpretations.

Taking this into account, this work takes the position that terrorism has a social meaning in society. Within this social meaning, there is a social construction of reality where "moral meanings ascribed to people or events are situationally dependent" (Wardlaw, 1990, 5). In this sense, terrorism is rather subjective. But, assuming we did have a clear definition of what terrorism is, can it ever be justified? (Miesels, 2008, 30). Without grounds for justification, one cannot positively separate terrorism from legitimate action against oppression, marginalization or neglect. Without knowing the difference, it will continue to elude comprehension.

Notwithstanding the above discussion, the conventional perspective on terrorism argues that there is something called terrorism that constitutes a threat and risk to the public good and that states and societies need to consider and plan for it.

2.3. TERRORISM FROM A CRITICAL TERRORISM STUDIES PERSPECTIVE

Further to the above perspective, Critical Terrorism Studies (CTS) has emerged as a study that approaches terrorism from an alternative, broad perspective addressing the role of states and government agencies in using violence against their own citizens, or citizens of foreign countries (Lutz, 2010, 31). The advantage of this perspective is that it attempts to identify acts of political violence that are "terroristic" in nature without imposing pre-determined conceptual limits on which acts may qualify as terrorism perpetrated by state or non-state actors occurring during peace or war (Jackson, 2009, 14).

Essentially, CTS seeks to challenge the 'bias' that exists within conventional terrorism studies. According to Richard Jackson, these biases include:

- The propensity to focus on states and groups that Western states oppose;
- The failure to contemplate actions practiced by allies of Western states as having a terroristic nature;
- That terrorism is a major threat to international security; and
- That terrorists are mentally unstable (Jackson, 2008).

By challenging the above, CTS maintains a larger interdisciplinary framework than conventional terrorism studies. Perhaps one of the main differences between the two fields of study is the concept of 'us' versus 'them' – a concept which CTS is portrayed as dispelling, and which conventional terrorism studies appears to provoke. As we move forward in this work, this concept will become increasingly relevant in determining how one gauges responsibility in the outcome of events.

Given the modern day threat spectrum, it would be a very delicate matter to tread upon if one were to choose either side as being the sole answer to research on terrorism. There are far too many variables and intelligence gaps (unknown alliances, insider threats,

sabotage, espionage, etc) that exist for the author of this work to fully subscribe to one single point of view.

It cannot go without recognition that states play a significant role in both increasing and reducing its vulnerability to terrorism. Similar to how methods of prevention are brought about through policy and legislation, so to are vulnerabilities. As such, the author believes that terrorism is a rather complex area of study that should not be limited to one particular point of view. However, there is a scale for everything, which is why this work *mostly* agrees with the positions of CTS, but still acknowledges certain views that originate from conventional terrorism studies. In particular, the author appreciates how critical terrorism studies endeavors to reveal that the gap between

> Those who hate terrorism and those who carry it out, those who seek to delegitimize the acts of terrorists and those who incite them, and those who abjure terror and those who glorify it – is not as great as it is implied or asserted by orthodox terrorism experts, the discourse of governments, or the popular press (Booth, 2008, 66).

However, in a number of instances, this gap may also be much more complex than it appears, which is why it is still essential to keep in mind the positions held by conventional terrorism researchers. Further to this, because terrorism itself is a rather subjective topic, it is difficult to limit oneself to a single point of view.

In particular, the perspective of critical terrorism studies will be valuable when discussing the Walkerton case study in Chapter 5 of this work. Not only will it provide an alternate approach to what occurred there, but it will also serve to open up the discussion to issues that may not be traditionally viewed as a threat: privatization and neoliberalization. “Under neoliberalism everything either is for sale or is plundered for profit” (Giroux, 2005, 2). This notion is the foundation for the critical terrorism studies perspective on closing the

gap between what is, and what is often not understood to be an act of terrorism. As such, Walkerton is a unique case study since it represents a pivotal point where the benefits of neoliberalization were called into question. Not only does it showcase the failure of water infrastructure to detect a harmful substance, but it also calls into questions the benefits *and* harm of both centralized and decentralized control of public goods.

CHAPTER 3 WATER INFRASTRUCTURE SYSTEMS

Generally speaking, the current dominant water infrastructure systems are comprised of the supply/source (raw water), raw water transmission pipes, the treatment systems, the distribution systems (Ahmadi, 2010, 4414), and finally, the operational control systems that make it all possible (i.e. SCADA). Of course, once the water is used, it enters the wastewater infrastructure system, which is essentially comprised of collection and treatment facilities, and again operational control systems. Figure 1 below illustrates this cycle.

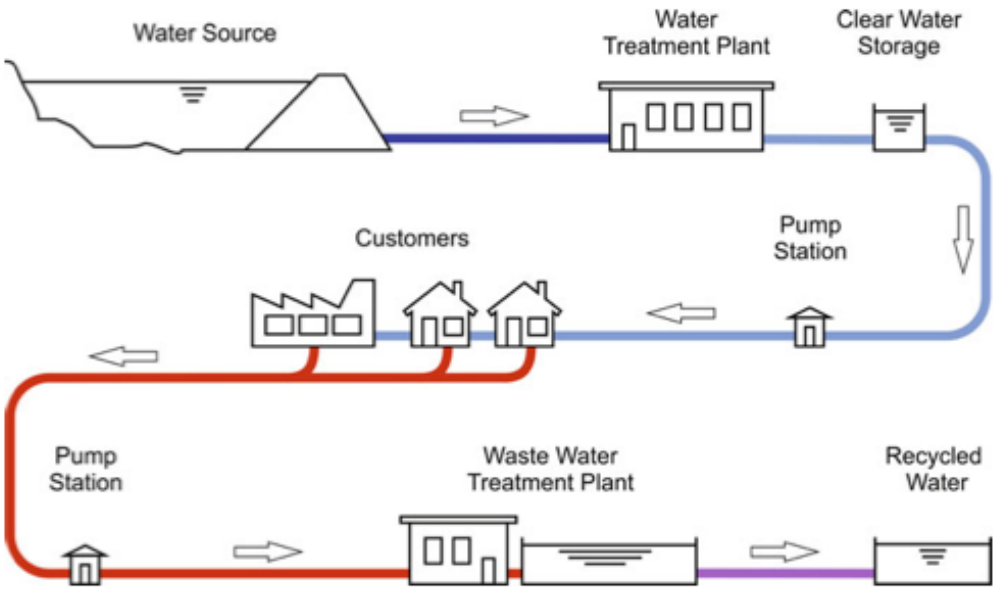


FIGURE 1: TYPICAL WATER DISTRIBUTION AND WASTEWATER COLLECTION SYSTEM SCHEMATIC
SOURCE: (BIRKETT, 2011, 458).

As depicted above, there are many parts and points to the entire water infrastructure system. With respect to this, the potential vulnerable areas have been identified as follows:

> "(1) Water sources, (i.e. river, reservoir, and wells);
> (2) Water treatment plants that remove impurities and harmful agents and make water suitable for domestic consumption and other uses;

(3) Water distribution pipelines that deliver clean water on demand to homes, commercial establishments, and industries;

(4) Storages (tanks); and

(5) Other facilities" (Hasestad, et al, 2003, np).

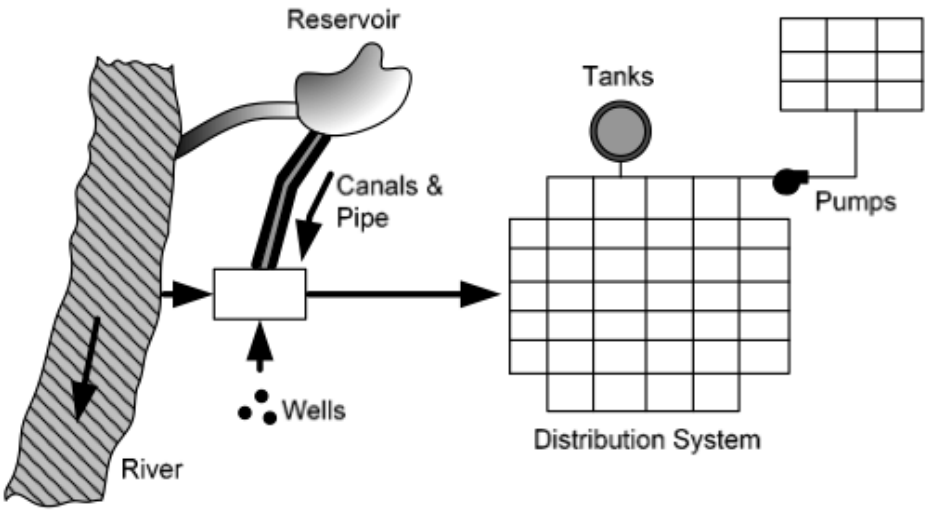


FIGURE 2: ELEMENTS AND VULNERABLE POINTS IN A GENERAL WATER SUPPLY SYSTEM
SOURCE: (HASESTAD, ET AL 2003, NP).

As Figure 1 and 2 both illustrate, the water infrastructure is comprised of both natural and technological elements to serve its customers. The following sections within this chapter will go into further detail about the most critical portions of this infrastructure.

3.1 (RAW) SOURCE WATER

Sources where water is derived from are very diverse and differ for every municipality. Often, they include lakes, deep wells, rivers, and, in some cases, recycled sewage water. Depending on the availability of source water, some municipalities may depend on a combination of sources (Kroll, 2013, 5) to serve their population. Toronto's water supply is obtained from Lake Ontario.

Evidently, water sources usually cannot be attacked physically, per se[7]. However, depending on the size of the area the source water is obtained from, it may be vulnerable to contamination. Simply put, you cannot guard every single point of a lake or a river; it would neither be possible, or cost effective. While larger water sources have a built-in safeguard against intentional contamination (employees in the water industry refer to this as "the solution to pollution is dilution"), (Kroll, 2013, 5) smaller sources are much more vulnerable. Nevertheless, water sources can also be said to have a safeguard alongside dilution: sunlight. This is because potential contaminants must be suitable for dissemination in water: they must be "viable, dissolvable, stable, and transportable" (Gleick, 2007, 16). Although overcoming this obstacle is difficult, it is not impossible[8].

3.2 TREATMENT PLANTS

As indicated above, Toronto obtains water from the Lake Ontario. From here, pipes transport it to one of four treatment facilities: R.C. Harris Water Treatment Plant, F.J. Horgan Water Treatment Plant, R.L. Clark Water Treatment Plant, or the Island Water treatment Plant[9] (City of Toronto, 2014).

Water treatment plants are unique in the sense that for the most part, they represent the final barrier between contamination (accidental, deliberate or natural) and the customer (Kroll, 2013, 6). Therefore, the treatment plant is said to be the final stage where monitoring for any potential contamination occurs. As a result of this, treatment plants present an opportunity to impose a varying degree of harm. With keen knowledge of this, Al Qaeda (and perhaps others) have displayed interest in the DCS and SCADA devices

[7] Unlike untreated water storage tanks. However, according to Kroll, contaminating untreated water storage tanks is unlikely, but nuisance attacks may be more likely (Kroll, 2013, 6).
[8] For example: (1) Lake Superior: Mercury Poisoning (Copeland, et al, 2012, 1); and (2) Grassy Narrows 1969 (Rivers in Sarnia, Ontario) (Harada, et al, 2011, 1).
[9] For statistics on the four treatment plants, please see Appendix 2.

(which are utilized as operational control systems) for the purpose of disabling or disrupting the monitoring and control capability these system offer (Hildick-Smith, 2005, 7).

With regards to the above, perhaps an important feature to keep in mind during the treatment process, is that various chemicals are intentionally added to the water[10] (Kroll, 2013, 6). Considering this factor along with the knowledge that terrorist groups such as Al Qaeda have expressed interest in recruiting skilled individuals for the purpose of attacking water infrastructure systems (Poulsen, 2002), one may consider the outcome of deliberately releasing a large amount of potentially toxic content into the entire system! To think of this from an alternate perspective, Kroll explains that the potential adversary may not even have to infiltrate the treatment facility itself. He argues that it may be much simpler to infiltrate one of the companies responsible for delivering chemicals to the treatment plant,[11] or, to simply increase the dosage of usually benign chemicals up to toxic levels (Kroll, 2013, 6). Attending to such an issue as this may be problematic especially considering that such an incident may be realized by an external or internal source. Chapter 4B.3 will discuss this further in the section regarding *cyber threats*.

3.3 DISTRIBUTION SYSTEM

In brief, the distribution system within the water infrastructure system is comprised of an entire network of pipes, valves, pumping stations, reservoirs, and elevated tanks, to name a few (City of Toronto, 2014). Toronto's water distribution network is basically made up of four treatment plants, eighteen pumping stations, ten reservoirs and four elevated

[10] This may include flocculating agents, caustics, acids, and disinfectants, among others (Kroll, 2013, 6).
[11] The fear here being that one may be able to contaminate or replace the usual shipment with a toxic compound and deliver it to the plant as normal for the plant operators to add to the treatment cycle. Instead of 'cleaning' the water, they would be poisoning the finished water (Kroll, 2013, 6).

tanks that are each monitored by the Transmission Control Centre via a computerized process control system[12] (City of Toronto, 2014).

Widely acknowledged as the most vulnerable element in the water infrastructure network, the distribution system poses the greatest concern to public safety. Not only is this because monitoring for contaminants hardly exists, but the potential for dilution is greatly reduced, along with the time available to respond (Kroll, 2013, 7).

According to Kroll, the most likely scenario for an attack on the distribution system (if the goal is to inflict mass casualties), is to mobilize a backflow contamination incident utilizing a pump:

> A backflow attack occurs when a pump is used to overcome the pressure gradient that is present in the distribution system's pipes. This can be easily achieved by using pumps available for rent or purchase at most home improvement stores. After the pressure gradient present in the system has been overcome and a contaminant introduced, siphoning effects act to pull the contaminant into the flowing system. Once the contaminant is present in the pipes, the normal movement of water in the system acts to disseminate the contaminant throughout the network affecting areas surrounding the introduction point. The introduction point can be anywhere in the system such as a fire hydrant, commercial building, or residence. Some areas, however, are more vulnerable than others. Access points near high flow areas and larger pipes would be favored because they would disseminate the material to a wider area more quickly; however, any point except for those at the very end of long deadhead lines could be used to effectively access the system (Kroll, 2013, 7).

[12] "The computer system, overseen by a Pumping Control Officer, provides information on water pressures, flows, storage reservoir levels and chlorine residuals, as well as water and power consumption. In addition, equipment performance, flood conditions, temperatures in buildings and unauthorized entry are monitored. The Pumping Control Officer can control the operation of each pumping station and system valve operations to keep a proper balance between supply and demand while maintaining sufficient water pressure throughout" (City of Toronto, 2014).

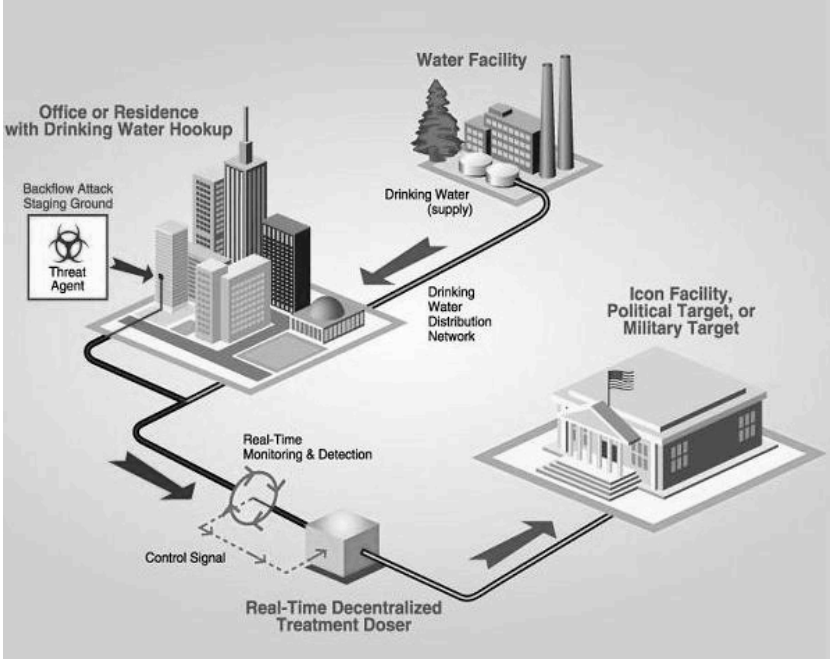


FIGURE 3: IMAGE DEPICTING THE VULNERABILITY OF DISTRIBUTION SYSTEMS TO BACKFLOW ATTACKS.
SOURCE: (KROLL, 2013, 8).

In recognition of the above vulnerabilities, the most likely compounds of concern, according to Kroll, are: heavy metals, herbicides, insecticides, nematocides & rodenticides, industrial chemicals & miscellaneous agents, illegal drugs, radionuclides, commercial products, chemical warfare agents, toxins and biogents (Kroll, 2013, 8). Further details of these agents are provided in Appendix 3.

On account of monitoring within the distribution system, two types of detection systems are used: toxicity monitoring and multi-parameter monitoring. Although each of these presents great benefits, there is also a problem in their use. In regards to toxicity monitoring, the tests used are proficient in identifying chemical toxins, but are largely ineffective in detecting biological agents (i.e. bacteria and viruses) (Kroll, 2013, 11). On the other hand, multi-parameter monitoring can detect a much larger assortment of potential threat agents from metals to organics to bio-agents (Kroll, 2013, 13). However, every

instrument has its disadvantages. In particular, these instruments are costly and require a large site for deployment, and many of these instruments generate a waste stream that would need to be managed (Kroll, 2013, 14).

3.4 WASTEWATER SYSTEM

Although Toronto's water treatment enterprise began in 1843[13], it was not until 1910 that construction began for Toronto's first wastewater treatment system at the southern tip of Leslie Street (Toronto, 2014). Then referred to as the Main Treatment Plant, it treated a capacity of 150,000 cubic metres of wastewater per day (Toronto, 2014). Today, we refer to this plant as the Ashbridges Bay Wastewater Treatment Plant, and there are three others that provide the same service: North Toronto Wastewater Treatment Plant, Highland Creek Wastewater Treatment Plant and the Humber Wastewater Treatment Plant – each of which are owned and operated by the City of Toronto (Toronto, 2014).

Without question, wastewater constitutes a significant threat to public health. It includes the mixture of both solid and liquid waste from residents and businesses that travel through a city's sanitary sewer system until it arrives at the wastewater treatment plant (Toronto, 2014). However, similar to the water supply system, wastewater treatment involves comparable provisions: collection, treatment, discharge systems and the control systems within these stages. This is further broken down in Figure 4 on the following page.

[13] The Toronto Gas, Light and Water Company (private corporation), began to distribute water through a small scale distribution system made out of wooden pipes to citizens who could afford the cost of the service…It was not until 1872 that City Council obtained passage of an act to form a publicly administered water works service (Toronto, 2014).

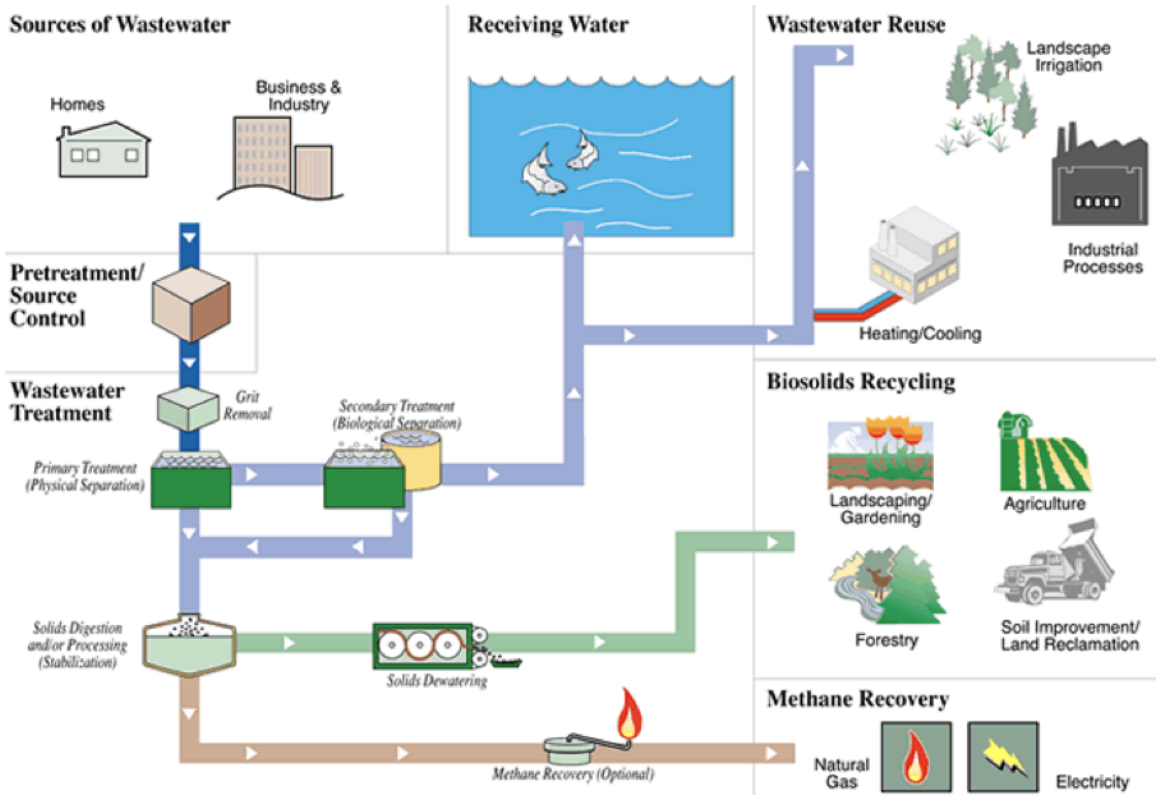


FIGURE 4: OVERVIEW OF WASTEWATER TREATMENT SYSTEM
SOURCE: (TORONTO, 2010).

If not anything else, the image above illustrates the potential hazards involved in transporting wastewater. In this case, providing physical and cyber security will be critical to coping with potential threats. This topic will be further discussed in the case studies section of this work.

3.5 SYSTEM OVERVIEW

As the sections in this chapter have indicated, the dominant water infrastructure system contains strengths and weaknesses. Thus far, this work has identified the systems involved in the treatment of water and wastewater systems. In the following, this work will explore how these threats may be realized.

CHAPTER 4 CONVENTIONAL TERRORISM STUDIES PERSPECTIVES ON WATER SECURITY ISSUES

In the post 9/11 world, conventional terrorism studies have become increasingly popular. Terrorists are seen as lurking everywhere and it appears that everything, to some extent has been *securitized*. Environmental security, food security, energy security and human security are a few of the many examples available. However, to some degree, each one of these relates back to the notion of *water security*. Although this term may be used to describe drought and water pollution, these aspects of water security fall out of the scope in conventional terrorism studies. Conventional terrorism studies typically focus what legal scholars refer to as the *actus reus* and *mens rea*: the act and the intent to exploit water infrastructure systems and networks for malicious[14] purposes.

PART A: SOURCES AND HAZARDS

4A.1 THREAT SOURCES AND HAZARDS

Terrorist threats to water systems are typically grouped into three sources: (1) External; (2) Internal; and (3) Miscellaneous (Van Leuven, 2011, 34). These sources are further broken down in Figure 5 below.

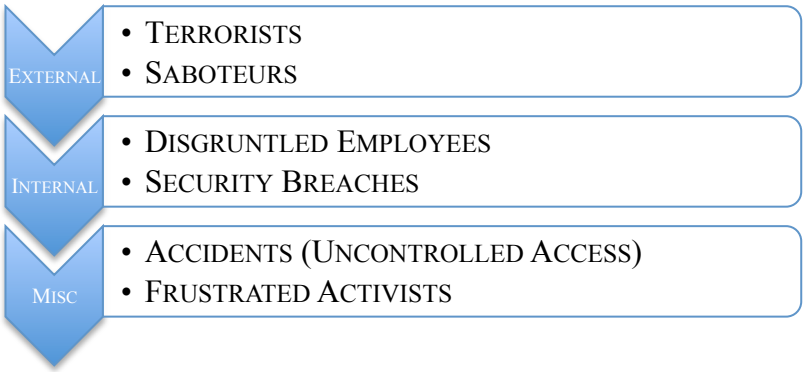


FIGURE 5: POSSIBLE THREAT SOURCES
SOURCE: (VAN LEUVEN, 2011, 34).

[14] For example, with the intention to cause harm (Merriam-Webster, 2014).

Considering the threat sources on the previous page, the hazards and threats to a water supply system may be broken down as follows:

HUMAN RELATED THREATS	▪ PHYSICAL DISRUPTION OF SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) NETWORK ▪ ATTACKS ON CENTRAL CONTROL SYSTEM TO CREATE SIMULTANEOUS FAILURES
CYBER THREATS	▪ ELECTRONIC ATTACKS USING WORMS AND VIRUSES ▪ NETWORK FLOODING ▪ JAMMING ▪ DISGUISING DATA TO NEUTRALIZE CHLORINE OR ADD NO DISINFECTANT, ALLOWING ADDITION OF MICROBES
PHYSICAL THREATS	▪ PHYSICAL DESTRUCTION OF SYSTEM'S ASSETS OR DISRUPTION OF WATER SUPPLY IS MORE LIKELY THAN CONTAMINATION ▪ LOSS OF WATER PRESSURE COMPROMISING FIREFIGHTING CAPABILITIES AND COULD LEAD TO POSSIBLE BACTERIAL BUILD-UP IN THE SYSTEM ▪ POTENTIAL FOR CREATING A WATER HAMMER EFFECT BY OPENING AND CLOSING MAJOR CONTROL VALVES AND TURNING PUMPS ON AND OFF TOO QUICKLY, WHICH COULD RESULT IN SIMULTANEOUS MAIN BREAKS.
CHEMICAL/BIOLOGICAL THREATS	▪ HEATH PROBLEMS, OR DEATH OF CUSTOMERS ▪ PANIC ▪ LOSS OF PUBLIC CONFIDENCE

TABLE 2: HAZARDS AND THREATS TO A WATER SUPPLY SYSTEM
SOURCE: MODIFIED FROM (AHMADI, ET AL, 2010, 4416).

4A.2 WHY ATTACK THE WATER INFRASTRUCTURE?

Exemplified in Table 2, an intentional attack on water infrastructure systems has the potential to yield dire results. Although recognition of the potential devastation has been acknowledged, questions such as 'the system has never been attacked before, why would it be attacked now?' not only cast doubt on the likelihood of an attack, but creates a problematic perspective blind to the reality that risks to water systems are increasing as a

result of an evolving threat environment (Van Leuven, 2011, 29), and the inability to adapt to change[15].

The potential to attack the water sector is certainly not new. In 1941, the Director of the Federal Bureau of Investigation, J. Edgar Hoover stated, "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" (Hoover, 1941, 1861-1865). What Hoover is discussing is the notion of interdependency, and most especially today, interconnectivity.

Increasingly, water infrastructure systems have become controlled and automated from remote locations in the name of efficiency. Additionally, this infrastructure relies on services provided by other critical infrastructures. This creates a 'system of systems' where a failure in one infrastructure has the capability of *cascading*, resulting in a disruption or failure to other critical infrastructures, and ultimately having consequences that could affect public health and safety, the economy, the government, national security, and finally, public confidence (Bahadur and William, 2011, 67). To illustrate this further, Figure 6 on the next page maps the interdependencies of the water sector.

[15] This is especially true in regards to how IT specialists and Industrial Control System (ICS) operators conflict on their views of security. Please refer to Appendix 7 for further information

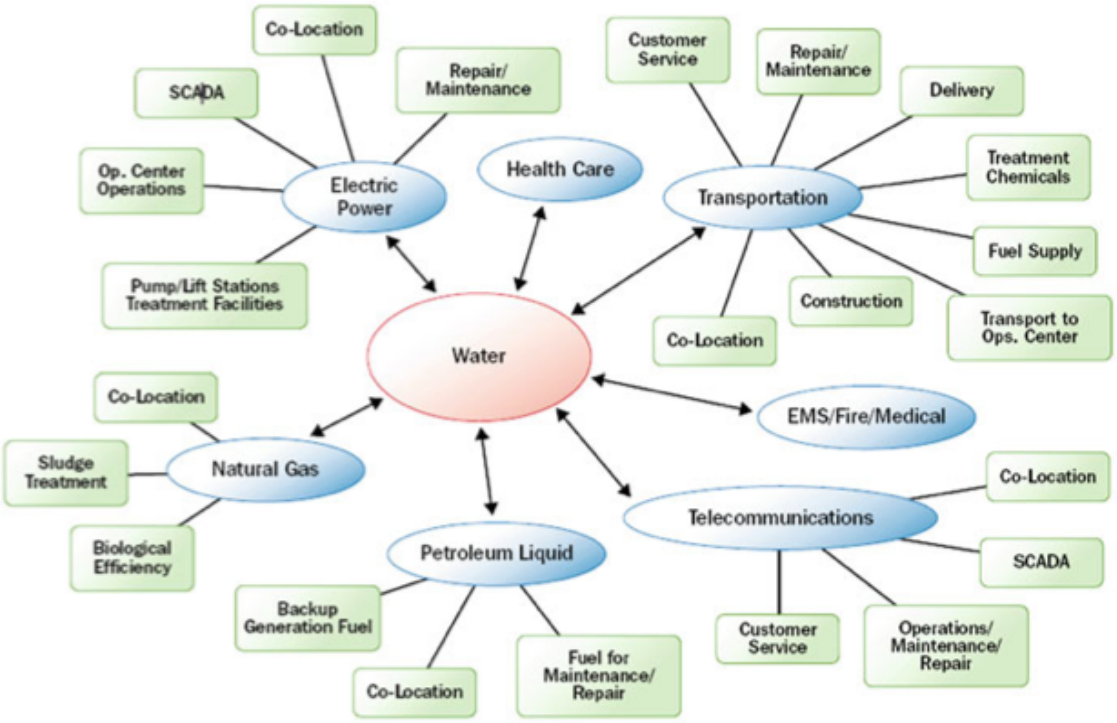


FIGURE 6: INTERDEPENDENCIES WITH THE WATER SECTOR
SOURCE: (DHS, 2007).

As depicted above, it is evident that the water infrastructure has a number of nodes to it. Some of these nodes may be of interest for an indirect, or direct attack opportunity. Some of these vulnerabilities will be discussed in the upcoming chapters.

4A.3 CONTAMINANTS OF CONCERN

Amongst a number of security issues pertaining to water is contamination, which may be realized through a physical or cyber attack. Although chemical and biological agents may evidently be less effective[16] as water threats, such agents are *potentially* capable of causing casualties (Bahadur and William, 2011, 70). According to Deininger, a contaminant must meet the following criteria in order for it to be an effective threat:

[16] This is highly dependent on the type of toxin or pathogen used, and moreover, the quantity and quality used.

- "High toxicity–deadly effect in small amounts
- No taste or odor
- Chemical and physical stability
- Delayed action to protect the sabotage agent
- Difficult recognition of poisoning – no specific pathologic changes in the organism
- Difficulties with the detection of the poison with normal analytical methods
- Unusual effects of poison; no known antidotes" (Deininger, 2000, np).

In addition to the above, knowledge of the infrastructure system – either physically or via a cyber means – is also necessary as this will be the final barrier to achieving the end state of a potential attack. Surely, knowledge of the vulnerabilities of the water infrastructure system as a whole will be critical to success at this point. So, the next question is: what is the water infrastructure system comprised of, and, do any vulnerabilities exist?

4A.4 SUMMARY OF THOUGHTS

This chapter, using a conventional terrorism studies lens has illustrated a number of security issues pertaining to water infrastructure systems. As alluded to earlier, there are a number of threat sources and hazards that have been identified as the potential means of an attack. But, this still begs the question, why would anyone want to attack water infrastructure systems? Further to this, who would carry out such a heinous action? Should all attacks upon infrastructure be observed through the lens of terrorism? What action or 'use of force' would constitute an attack? Moreover, how does one define attack? Does an attack always consist of a direct action, or can indirect action contribute to its definition?

Answering these questions can be an entire book on its own. Although it is not the objective of this work to answer each of the above questions, they constantly remain on the conscience of the author. Earlier on, it was brought forward that terrorism is a subjective topic, and it is difficult to limit oneself to viewing it through the conventional *or* critical

studies lens. Essentially, both are required to provide a holistic comprehension on the issues of defining and understanding terrorism, and furthermore, defeating it. Both conventional and critical terrorism studies will require one to consider the "roots" of terrorism. While the conventional study will often assess the "terrorists" personality, critical terrorism studies will take a step back and ask the bigger questions: *who* is this individual?; *why* did this individual commit this action?; *what* provoked him/her?; and so on. In sum, critical terrorism studies is interdisciplinary in that it seeks to analyze the roots more so than conventional terrorism studies. This is crucial since understanding the roots of terrorism will essentially allow one to understand *why* acts of terrorism occur, and moreover, present an opportunity for terrorist attacks to diminish in frequency and severity.

Perhaps of increasing concern are the ongoing threats put forward by ISIS since mid autumn 2014. Although the attacks thus far have been carried out by ISIS sympathizers, and have been relatively simplistic in terms of weaponry, the positive identification of an ISIS laptop (in August 2014) describing how to develop biological weapons - among other things – indicates the interest in carrying out complex attacks. At the very least, the nature of this circumstance should prompt a review of current infrastructure security issues, and furthermore, an attempt to resolve them.

Alas, we can return to the question posed earlier: What is the water infrastructure comprised of, and, do any vulnerabilities exist?

PART B: THE THREAT

Before we begin this part of the chapter, a schematic of the threats to the entire water infrastructure system is provided on the following page with a view to map out the overall threats to the water supply system as a whole.

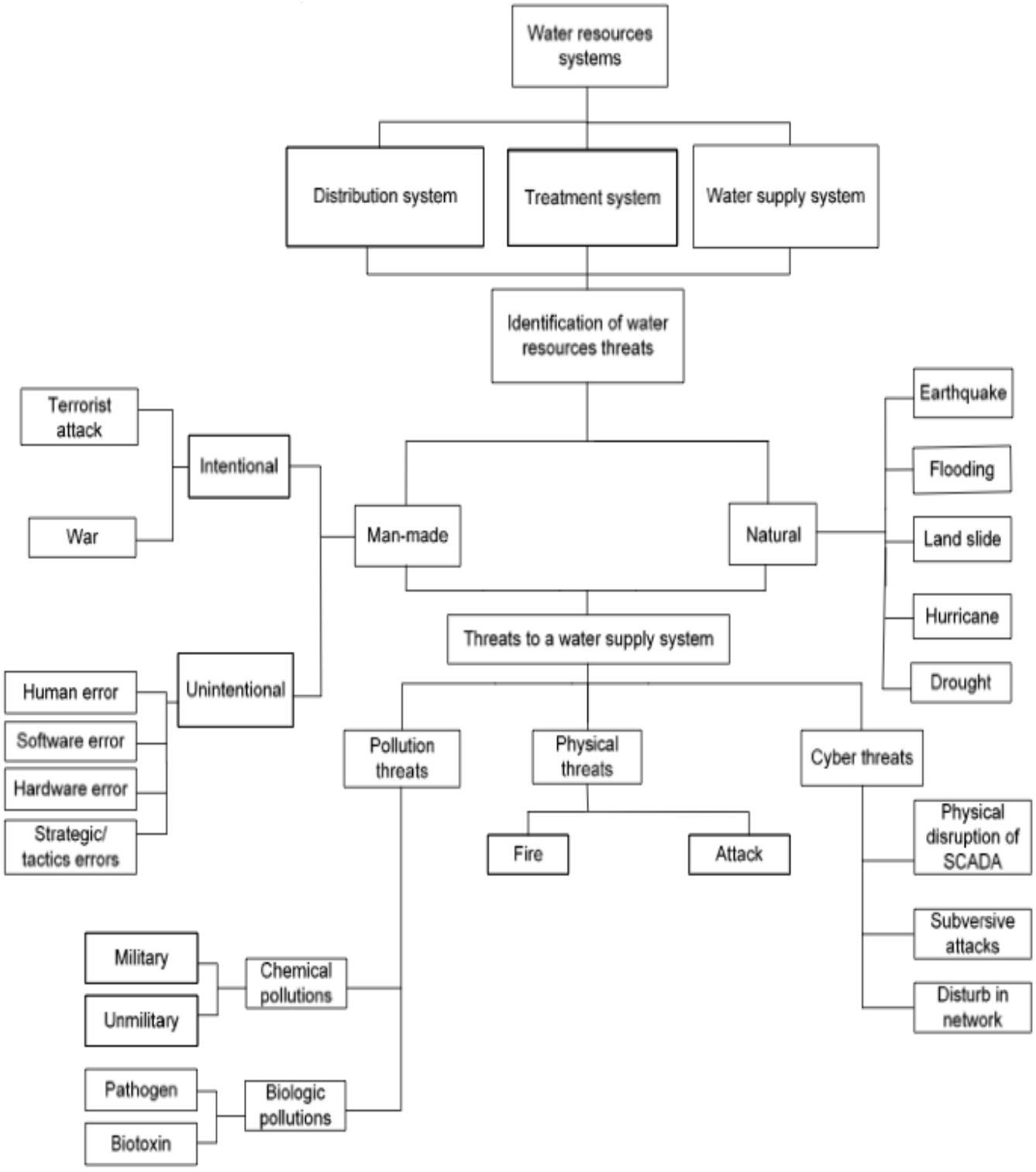


FIGURE 7: HAZARD AND THREATS TO A WATER SUPPLY SYSTEM
SOURCE: (AHMADI, 2010, 4417).

4B.1 BIOLOGICAL THREATS

As alluded to in previous sections, biological threats to water infrastructure are highly dependent on the concentration of the toxin or pathogen in the water[17]. It is for this reason that source water is not as much of an ideal threat as treatment plants, storage facilities and especially the distribution system. First and foremost, the addresses for each of these locations are readily available on the City of Toronto's website (City of Toronto, 2014). So, how can a biological threat be realized?

Before we divulge into this question, it is necessary to understand that biological agents fall into two separate categories: toxins and pathogens[18]. Table 3 and 4 below will identify the biological toxins and pathogens that are considered water threats:

PATHOGEN	TYPE	WEAPONIZED	STABLE IN WATER	CHLORINE TOLERANCE
ANTHRAX	B	YES	2 YEARS SPORES	SPORES RESISTANT
BRUCELLOSIS	B	YES	20-72 DAYS	UNKNOWN
CLOSTRIDIUM PERFRINGENS	B	PROBABLE	COMMON IN SEWAGE	RESISTANT
TULAREMIA	B	YES	<90 DAYS	INACTIVATED, 1 PPM, 5 MIN
SHIGELLOSIS	B	UNKNOWN	2-3 DAYS	INACTIVATED, 0.05 PPM, 10 MIN
CHOLERA	B	UNKNOWN	YES	"EASILY KILLED"
PLAGUE	B	PROBABLE	16 DAYS	UNKNOWN
Q FEVER	R	YES	UNKNOWN	UNKNOWN
HEPATITIS A	V	UNKNOWN	UNKNOWN	INACTIVATED, 0.4 PPM, 30 MIN

NOTES: B, BACTERIA; R, RICKETTSIA; V, VIRUS
TABLE 3: BIOLOGICAL PATHOGENS CONSIDERED WATER THREATS
SOURCE: MODIFIED FROM (GLEICK, 2007, 20).

[17] Biological threats do not pose a serious risk to wastewater utilities as treated sewage is not consumed in Canada (Sauder, 2010, 13)
[18] Toxins are "chemicals derived from the natural metabolic processes of organisms", while pathogens are live organisms "such as bacteria, viruses or protozoa" (Hickman 1999).

TOXIN	WEAPONIZED	STABLE IN WATER	CHLORINE TOLERANCE
BOTULINUM	YES	YES	INACTIVATED AT 6 PPM, 20 MIN
T-2 MYCOTOXIN	PROBABLE	YES	RESISTANT
AFLATOXIN	YES	PROBABLE	RESISTANT
RICIN	YES	UNKNOWN	RESISTANT AT 10 PPM
STAPHYLOCOCCUS ENTEROTOXINS	PROBABLE	PROBABLE	UNKNOWN
MICROCYSTINS	POSSIBLE	PROBABLE	VERY RESISTANT AT 100 PPM
ANATOXIN A	UNKNOWN	INACTIVATED IN DAYS	UNKNOWN
TETRODOTOXIN	POSSIBLE	UNKNOWN	INACTIVATED, 50 PPM
SAXITOXIN	POSSIBLE	YES	RESISTANT AT 10 PPM

TABLE 4: BIOLOGICAL TOXINS CONSIDERED WATER THREATS
SOURCE: MODIFIED FROM (GLEICK, 2007, 21).

As depicted above, there are a number of toxins and pathogens that remain resistant to chlorine treatment. Given this, it is evident that bioagents may pose a notable threat to water infrastructure systems [19]. Although most research on 'bioterrorism' and water infrastructure systems cite major barriers and drawbacks to those who may attempt to poison the system[20], much of these studies fail to account for the fact that little to no monitoring is done at the distribution stage, and where monitoring does occur, how quickly a response occurs before the affects are felt by the population.

A successful attack utilizing bioagents may occur as a result of a physical attack (ie. A backflow attack), or a cyber attack, which will be discussed later in this chapter. For

[19] However, it is also key to mention that information is not readily available on how these pathogens and toxins are affected by the newer, non-chlorine based water treatment systems, such as ultraviolet disinfection, ozonation, and advanced filtration (Gleick, 2007, 21)
[20] For example, dilution, chlorine

example, Hickman cites that only 0.21 kilograms of Botulinum Toxin is necessary to effectively contaminate a 750,000 litre storage facility, and ingestion of only 250 millilitres would result in a disabling dose (Hickman, 1999, 1). Although the greatest task of using a biological agent on any part of the water supply systems is the ability to procure the agent (Sauder, 2010, 11), it is quite evident that significant damage can be done.

As discussed in previous sections, there is no *reliable* detection system for biological agents (Simon, 1997, 428-430). Even the multi-parameter monitoring has its setbacks in that it would likely not get the information out to the public in time to prevent casualties. This illustrates the reality that the only true monitoring that occurs after water leaves the treatment facilities is public health monitoring: if the population gets sick, there is likely a problem (Sauder, 2010, 11).

But just how real is this threat? Can it be realized? Ken Alibek[21], a former Soviet Biopreparat[22] Scientist has indicated that with the fall of the Soviet Union, a large number of scientists are unaccounted for. Dr. Alibek states the following:

> The services of an ex-Biopreparat scientist would be a bargain at any price. The information he could provide would save months, perhaps years, of costly scientific research for any nation interested in developing, or improving a biological warfare program. It is impossible to know how many Russians have been recruited abroad, but there is no doubt that their expertise has been attracting bidders. At least twenty-five former specialists in the Soviet Union's biological warfare program are now in the United States. Many more have gone to Europe and Asia or have simply dropped out of sight. I've heard that several went to Iraq and North Korea. A former colleague, now the director of a Biopreparat institute, told me that five of our scientists are in Iran. *The New York Times* reported in December 1998 that the Iranian government dispatched a 'scientific advisor' attached to the office of the presidency to Moscow to recruit former scientists from our program…Last year, *Top Secret* reported that a Biopreparat official turned up at the Chinese embassy in Moscow to offer his services…The West is also worried…the vulnerability of our biological arsenal should also raise concern. A vial of freeze-dried powder takes up less space

[21] Dr. Ken Alibek defected from the Soviet Union, and now resides in the United States.

[22] Biopreparat Labs were amongst one of the closest guarded secrets of the Cold War. It can likely be compared to Camp Detrick in Maryland, USA.

> than a pack of cigarettes and is easy to smuggle past an inattentive guard. It happened when I was at Biopreparat, when security was at its peak. Biological agents once kept secure in government facilities are rumored to be circulating freely in the Russian criminal underworld (Alibek, 1999,271-272).

Clearly, Dr. Alibek's statement is quite profound in that it illustrates expertise and evidently, uncertainty. Whether an attack is currently being planned is unknown, but statements such as his certainly force one to consider the possibilities.

4B.2 CHEMICAL THREATS

Similar to biological threats, chemical threats may also be classified into two types of agents: chemical weapons and industrial chemicals. Similar to biological agents, chemical agents may be difficult to produce – although this has changed with the advent of the Internet as a global information hub. Table 5 on the following page provides a rundown of the dose and solubility of chemical agents. Particular attention should be drawn to the point that a lethal chemical dose is vastly reduced compared to biological agents.

Very low doses of chemical agents have the potential to produce abrupt death (Hickman, 1999, 1)[23]. Industrial chemicals are the most likely agents to be used as they are widely available at innumerable sites across Canada (Sauder, 2010, 12). Perhaps the best example is Sodium Cyanide (used largely in the mining and metals industry). According to Hickman, "death or incapacitation can result from a 25mg oral dose" (Hickman, 1999, 1). A simple Internet search for 'sodium cyanide'[24] (NaCN) easily turns up suppliers for this product. It is an odorless white salt that is highly soluble and stable in water (approximately

[23] The Sarin attack in Japan's subway by Aum Shinrikyo in 1995 and the U.S. Anthrax attack in 2001 exemplify this.

[24] For example: http://www.alibaba.com/showroom/sodium-cyanide.html?uptime=20121129&ptsid=1013000015669012&crea=28367223020&plac=&netw=g&device=c&ptscode=0110202060010001

80 percent at 35 Degrees Celsius) (Hickman, 1999, 1). Hickman cites the following scenario:

> Thus, a saboteur with four and a quarter 100-pound "cement" bags of NaCN, with access to the clear wells, or storage bladders in the austere case, could generate a poisonous slug of water that could kill or incapacitate every consumer downstream. Properly timed, a "construction worker" could cripple operations through a relatively cheap and simple asymmetric attack (Hickman, 1999, 1).

Chemical Agents (milligrams per liter (mg/l) unless otherwise noted)	Acute Concentration[a]	Recommended Guidelines	
	0.5 L	5 L/Day	15 L/day
Chemical Warfare Agents			
Hydrogen cyanide	25	6.0	2.0
Tabun (GA, microgram/liter (µ/l))	50	70.0	22.5
Sarin (GB , µ/l)	50	13.8	4.6
Soman (GD, µ/l)	50	6.0	2.0
VX (µ/l)	50	7.5	2.5
Lewisite (Arsenic fraction)	100-130	80.0	27.0
Sulfur Mustard (µ/l)		140.0	47.0
3-quinuclidinyl benzilate (BZ, µ/l)		7.0	2.3
lysergic acid diethylamide (LSD)	0.050		
Industrial Chemical Poisons			
Cyanides	25	6.0	2.0
Arsenic	100-130	80.0	27.0
Fluoride	3000		
Cadmium	15		
Mercury	75-300		
Dieldrin	5000		
Sodium fluoroacetate[c]		None provided	
Parathion[c]		None provided	

Sources:
a. Major John Garland, *Water Vulnerability Assessments*, (Armstrong Laboratory, AL-TR-1991-0049), April 1991, 8-9. The author assumes acute effects (death or debilitation) after consumption of 0.5 L.
b. National Research Council, Committee on Toxicology, *Guidelines for Chemical Warfare Agents in Military Field Drinking Water*, 1995, 10. Listed doses are "safe."
c. W. Dickinson Burrows, J. A. Valcik and Alan Seitzinger, "Natural and Terrorist Threats to Drinking Water Systems," presented at the American Defense Preparedness Association 23rd Environmental Symposium and Exhibition, 7-10 April 1997, New Orleans, LA, 2. The authors consider the organophospate nerve agent VX, the two hallucinogens BZ and LSD, sodium cyanide, fluoroacetate and parathion as potential threat agents. They do not provide acute concentrations or lethal doses.

TABLE 5: VIABLE CHEMICAL AGENT OPTIONS (DOSE AND WATER SOLUBILITY)
SOURCE: ADAPTED FROM (SAUDER, 2010, 12).

To add to Hickman's scenario, it is important to note that there is limited monitoring obtainable for chemical threats because such tests are designed to monitor for specific compounds (Sauder, 2010, 13). Hickman further echoes this by citing that "chemicals do not have compounds that can be inactivated through current purification

methods" (Hickman, 1999, 1)[25]. Moreover, it can be stated that the vulnerabilities mentioned herein (within the treatment, storage and distribution network) can be quite easily exploitable with chemical agents, especially given the lack of effective monitoring.

4B.3 CYBER THREATS

Cyber threats pose a great risk to water infrastructure systems. This work has previously mentioned industrial/operational control systems such as SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems). Essentially, what these systems have accomplished is centralized control, which has had economic benefits for utilities. However, to the dismay of all computer users, even these systems have their shortfalls, and therefore produce additional vulnerabilities that increase the risk to water infrastructure.

Essentially, SCADA systems are comprised of three main components: field devices[26], servers[27], and client machines[28] (Sauder, 2010, 13). Although the SCADA system is utilized on its own Intranet, this only *limits*[29] the vulnerability of cyber exploitation. It does not render it completely secure. The best example of this is the Stuxnet worm which was designed to directly attack a particular Siemens SCADA system that happened to be in large-scale use in Iran's uranium enrichment facilities. Although there is much evidence that this worm was State-sponsored, its code has since been copied and is available online (Kaplan, 2011, 1). Additionally, other websites have released their own

---

[25] Likewise to biological agents, chemical agents do not pose a threat to the wastewater infrastructure as treated sewage is not consumed in Canada (Sauder, 2010, 13)

[26] "Field devices provide information and operational control to pumps, pressure, valves and other operations around the utility" (Sauder, 2010, 13)

[27] "Servers combine the information from the field devices and monitor it remotely to ensure all systems are running correctly, alarms are triggered if functions are not operating normally" (Sauder, 2010, 13)

[28] "Client machines are used for monitoring and user control of the entire system" (Sauder, 2010, 13)

[29] The term *limit* is used herein as it has been publically revealed that hacking into an isolated system using FM radio signals is possible. See "AirHopper" hack (Kumar, 2014).

versions of malicious codes that target SCADA and other system exploits. For example, the GLEG[30] exploitation kit offers 128 exploits as of version 1.17 (Chaney, 2012). Metasploit is also another website which offers similar exploitation kits (Chaney, 2012).

In addition to the above, many more vulnerabilities have materialized as a result of a multiplicity of means and improper actions. Consequently, threats and vulnerabilities will continue to emerge until more sophisticated security strategies are implemented. Appendix 4 further exemplifies SCADA Vulnerabilities.

As a result of the nature of such control/operational systems, effectively gaining control of the SCADA system would grant the saboteur operational access to the system. Essentially, the saboteur can effectively access, bypass, modify, or shutdown any number of programs or systems within the water infrastructure system (i.e. chemical or biological agents could be dispensed directly into the system (Shea & Library of Congress, 2004 ; Sauder, 2010, 13-14). Unlike biological or chemical agents, a cyber threat can also have implications to wastewater treatment facilities (i.e. Maroochy Wastewater Treatment Plant, Australia).

As we move forward into the twenty-first century, utilities are relying more heavily on systems that provide centralized control and data acquisition such as SCADA (Sauder, 2010, 13-14). Despite this, and the current 'off-the-shelf' exploit kits available, "there appears to be little market incentive to directly increase industrial control system security" (Shea & Library of Congress, 2004 ; Sauder, 2010, 14). Given the critical operational role SCADA systems maintain in the water and wastewater treatment process, it can be

[30] See http://www.gleg.net/ for further information

surmised that these systems present a huge vulnerability to the water infrastructure system as a whole[31].

4B.4 PHYSICAL THREATS

Physical threats to the water infrastructure system may employ the use of explosives, property damage, arson, and mechanical tampering (Van Leuven, 2011, 45) to name a few. Additionally, it has the likelihood of occurring from three threat sources: external (sabotage), external (criminal), and internal (disgruntled employee) (Van Leuven, 2011, 45). Table 6 below goes into further detail using the pump station as an example of an asset that would be physically attacked.

ASSET	THREAT	TACTICS	LIKELIHOOD OF SUCCESS
PUMP STATION	EXTERNAL, SABOTAGE	EXPLOSIVES, MECHANICAL TAMPERING, ARSON	*MEDIUM* – DEPENDING ON ACCESS CONTROL AND DETECTION CAPABILITIES
PUMP STATION	EXTERNAL, VANDAL OR CRIMINAL	GRAFFITI, PROPERTY DAMAGE, THEFT OR EQUIPMENT OR WIRE	*MEDIUM* – DEPENDING ON FENCES AND ACCESS CONTROL
PUMP STATION	INTERNAL, DISGRUNTLED EMPLOYEE	MECHANICAL TAMPERING OR ELECTRONIC PANELS	*HIGH* – EMPLOYEES HAVE ACCESS, KNOWLEDGE, AND OPPORTUNITIES

TABLE 6: POTENTIAL ASSET/THREAT COMBINATIONS
SOURCE: MODIFIED FROM (VAN LEUVEN, 2012, 45).

Additional examples of a physical threat to water infrastructure systems includes, but are not limited to the destruction of dams and distribution lines (Hickman, 1999, 1).

[31] For a SCADA Network attack Scenario, please refer to Appendix 5

Given that provinces under their own emergency management legislation[32] are tasked with protecting their critical infrastructure (Sauder, 2010, 14), it will be absolutely necessary for the City of Toronto (Utilities) and the Province to increase their partnership in continuing to secure the water and wastewater treatment facilities with a view to take into account the evolving threat landscape. To date, it appears as though the province or the federal government does not mandate vulnerability assessments specifically to the water sector in Canada (Sauder, 2010, 14). Interestingly enough, the United States is much different, including mandated vulnerability assessments, rigorous guidelines, and regulated security upgrades, each of which further contributes to improved disaster resilience (Katen, 2004, 16).

4B.5. SUMMARY OF THOUGHTS

Thus far, this work has discussed water security issues, the water infrastructure system, and the known biological, chemical, cyber and physical threats from a conventional terrorism studies perspective. It is important to recognize that these threats were not discussed in any type of chronological manner. It would be rather contentious to indicate that any one of these threats is more important than the other. Instead, the author recommends being mindful of how each may overlap and further to this, how the dynamic environment of the twenty-first century requires vigilance of a multitude of threat sources, some of which may be the result of poor planning.

The accidental discovery of vials of smallpox in a lab in the National Institute of Health in the United States in July 2014 prompted a 'hunt' for other highly poisonous substances (BBC, 2014) that may not have been stored properly. During this 'hunt', vials of

[32] In Ontario, this would be the *Ontario Emergency Management and Civil Protection Act*

poisonous substances including the plague, botulism and a rare tropical infection (BBC, 2014) were found. Although they had been safely sealed, officials had found that these deadly microbes were not stored properly, likely because they were part of a historical collection that was once allowed to be stored without regulation! (BBC, 2014). Incidents such as this probe further questions: how often does this happen? How many incidents similar to this have occurred that have not been reported? How many still exist? If no storage regulations exist for those microbes, how can one know if any vials are missing? One can ask endless questions on this matter, but the point here is rather simple: if something like this can happen (in the U.S.A. of all places!), what is the probability and possibility of it happening somewhere else?[33]

Again, this work is not about casting fear, uncertainty or doubt. It is about the identification and awareness of security issues within water infrastructure systems that exist in the dynamic threat environment of the twenty-first century. In Donald Rumsfeld's words, we are currently living in a time of "unknown unknowns," that is, ignorances which we do not even know we are ignorant of. Somewhere, someone may have already beaten us in a battle we had no idea we were fighting (Chatfield, 2012). It is exactly for this reason that Canada must further develop its means to secure its infrastructure.

PART C: CASE STUDIES

As both Table 1 and Appendix 1 illustrate, there has been a long history of attacking water systems. This chapter will therefore bring to the forefront case studies on Milwaukee, and the Maroochy Wastewater Treatment Plant in Australia.

[33] This question is of course, not limited to the discovery of biological microbes, but also to an array of other information or material. For example, improper chemical storage, improper password storage, improper equipment usage, etc.

4C. 1 MILWAUKEE

During the months of March and April of 1993, Milwaukee experienced the largest epidemic of waterborne disease in U.S. history (Infectious Disease News, 2007, 1). Beginning on March 23rd, hospitals and schools in Milwaukee began reporting staffing issues to the city's Department of Public Health when, suddenly, a large number of both nurses and teachers called in sick. During the initial two week period, it is estimated that approximately "403,000 people reported sudden acute watery diarrhea" (25% of the city's population) (Infectious Disease News, 2007, 1). In addition to this, approximately 100 people died of this waterborne outbreak, which was later identified as cryptosporidium – a protozoan parasite that causes gastrointestinal illness (Corso, et al, 2003, 426-431).

Although an increase in the water's turbidity was noticed at the city's Howard Avenue Treatment Plant, along with a large decline in the number of students at school (Gradus, Singh, and Sedmak 1994, 57-60) in late March, it was not until additional complaints reached the Department of Health on April 5th that tests had commenced. Finally, on April 7th, the Mayor ordered a boil water advisory to the city after laboratory tests confirmed cryptosporidium in the city's water (MacKenzie, et al. 1995, 57-62).

According to Gradus, Singh and Sedmark, residents of Milwaukee had consistently made contact with the city's water department, where complaints of cloudy, foul-smelling water was met by utility workers depositing more chlorine into the system in an attempt to fix the issue (Gradus, Singh, and Sedmak 1994, 57-60). Being resistant to chlorine, this attempt did not aid the problem at hand, but instead increased the length of time that the population was exposed to the parasite.

Although this incident was not an intentional attack per se[34], it is significant to this work in that it illustrates a population that was acutely vulnerable to a parasite as a result of poor monitoring and identification methods[35]. This particular parasite had entered the city's Howard Avenue Treatment Plant through an intake pipe in Lake Michigan, and by the time water utility workers understood what was going on, it was already too late: approximately 25% of the population fell ill, with 100 fatalities. Since this incident however, Milwaukee has become the leader in water quality in the United States (Golden, 2013, 1).

4C. 2 MAROOCHY WASTEWATER TREATMENT PLANT

From approximately February 9th to April 23rd of 2000, the Maroochy Wastewater Treatment Plant in Australia (approximately 100 kilometers North of Brisbane), utility workers had experienced a series of faults in the SCADA system of the plant (Weiss, 2010, 111). The individual behind the series of disruptions was a former site supervisor of Hunter Watertech who resigned from his position and approached the city council seeking employment (Weiss, 2010, 111). Infuriated with the city for turning down his job application, Vitek Boden decided to take matters into his own hands.

Utilizing stolen radio and computer equipment, Boden was able to successfully sabotage the control systems of the Plant, resulting in approximately 800,000 litres of

---

[34] A few weeks after the outbreak, the public had learned that the operators of the city's Howard Avenue Treatment Plant had lost full control of the treatment process in late March, which allowed the Cryptosporidium to break through the filters. The operators did not pay attention to the indicators of changing water quality that were in place at the time. The pathogen had been going through the city's water mains for more than two weeks before the boil-water advisory was announced (Behm, 2013).

[35] "Today, the turbidity, or cloudiness, of filtered water is measured constantly inside the plants. Turbidity is an indicator of the concentration of particles of all kinds suspended in water. Before April 1993, operators collected just one sample of water every eight hours from treated water in storage to be checked for turbidity. No one checked water leaving the filters. No particle counters were installed at either plant before the outbreak. Now, there are particle counters on each filter. They provide minute-by-minute counts of anything floating in filtered water and report the number of particles of different sizes, including a range of 3 to 5 microns that might indicate the presence of *Crypto*…From 1994 through 1998, the Water Works invested $89 million to upgrade the two filtration plants and bolster barriers to contamination of drinking water" (Behm, 2013).

untreated sewage released from various parts of the Maroochy Plant resulting in death to marine life, and the nearby creek water turning black with a stench that remained unbearable for residents (Abrams and Weiss, 2008, 8).

As indicated above, Boden had achieved his actions with a stolen radio and computer equipment. He was able to disable alarms at four pumping stations (Weiss, 2010, 111). While a Hunter Watertech investigator was attempting to troubleshoot the system, he had noticed that the log indicated that the program had been run at least thirty-one times. As a result of Boden's success in disabling the alarms at the selected stations, his actions went unnoticed for a period of time (Weiss, 2010, 111).

Unlike the previous two case studies, this is one which portrays deliberate and malicious intent. Internationally speaking, this incident represented one of the first successful SCADA system attacks. Moreover, it illustrates the capability of an individual with skilled knowledge to cause widespread disruption and damage from the outside.

PART D: INTERVIEWS

4D.1 INTRODUCTION TO SUBJECTS INTERVIEWED

Although much information has been obtained through the use of secondary sources, it is necessary to engage individuals within the field of security to truly understand if there is an imminent threat as well as the controversies situated in the threat environment. In an attempt to do that, contact was attempted with a number of representatives from:

- Toronto Water Integrated Technology Management Unit
- R.C. Harris Treatment Plant
- Defense Research and Development Canada – Suffield
- Biology Professors

- Chemistry Professors
- Carleton University Infrastructure Protection Program
- Public Safety Canada
- Ontario Clean Water Association
- The Pacific Institute (Think Tank)

Perhaps as a result of the sensitivity of the issue that was being discussed, the vast majority of those contacted either did not respond, or, offered referrals to other individuals who also did not respond. Of the many that were contacted, three individuals agreed to be part of the discussion.

- Joseph Weiss PE, CISM, CRISC, ISA Fellow, IEEE Senior Member, Applied Control Solutions, LLC (U.S.A.)
- Michael Goedeker, Sophos, HAKDEFNET (Computer & Network Security) (U.S.A.)
- An anonymous source from outside of Canada (Water: Business Strategy and Resilience) (personal responses).

4D.2 COMPARISONS, CONTROVERSIES AND DISCREPANCIES

The discussions with the participants of this study focused on whether or not current water infrastructure systems were at risk to either a physical, chemical, biological or a cyber attack.

In general, each of the individuals agreed that critical infrastructure is vulnerable to attack. For example, Joe Weiss argued that there are always “three legs to security”: physical security, IT security and ICS security. However, despite current attempts, all ICS (Industrial Control Systems, i.e. SCADA) are vulnerable to cyber attacks, no matter what

industry they are in (Weiss, 2014; Weiss, 2010). As a result of this, contamination of various parts of the water infrastructure system are in fact possible. Although this is quite comparable to what has been illustrated in this work thus far, the anonymous source brought in an interesting perspective as well.

In discussing risk and vulnerability of water infrastructure systems, the anonymous source believed that water systems are at risk of attack from malware, insiders, hackers, terrorist organizations, etc, especially in recognition of environmental change that may or may not create security issues themselves for water resources (Anonymous, 2014). This individual went on to state that the risk for water systems is more likely at the consumer end as the volume of contaminate required to conduct an attack at the bulk water end is much too great: the dilution effect mitigates the risk (Anonymous, 2014). When asked about the specific threats towards water infrastructures, the individual responded by citing that water supplies have been targeted for well over 2000 years (Anonymous, 2014). While modern systems are reasonably robust, and have redundancy built in for regular maintenance purposes, this individual recognizes that the cyber risk is increasing as organizations move to Internet based control and monitoring (Anonymous, 2014).

On the specific subject of the risks of a chemical or biological attack on the water infrastructure, the individual assessed the risk to be low for the sheer reason that better outcomes can be achieved by using the available resources to target mass crowds, for example, on railways or at sporting events (Anonymous, 2014).

Regarding the challenges in protecting water infrastructure, the individual again focused on the issue of cyber attacks becoming a larger issue in the long term as it would be possible to cause extensive damage in changing the dosage of chemicals, or as another

example, suddenly closing valves (Anonymous, 2014). The risk with this being that water systems have mass energy in moving water that 'does not go well' with sudden valve closers, which would result in thousands of tones of pressure impacting the system.

While on the subject of risk, this individual was also asked to shed light on how Al Qaeda's attempts to obtain information related to SCADA water systems has changed the way in which water infrastructures are secured. The individual's response indicated that post 9/11, water companies globally undertook extensive upgrades at key nodes such as treatment plants. However, as alluded to earlier on in this work, it is not possible to have a secure pipe network given the nature of the distribution system (Anonymous, 2014).

Taking into consideration all that has been said, Michael Goedecker was asked to speak to the topic of hacking. Without hesitation, Mr. Goedecker explained that there were six common steps most attackers use to find and exploit vulnerabilities in a given system. They include the following:

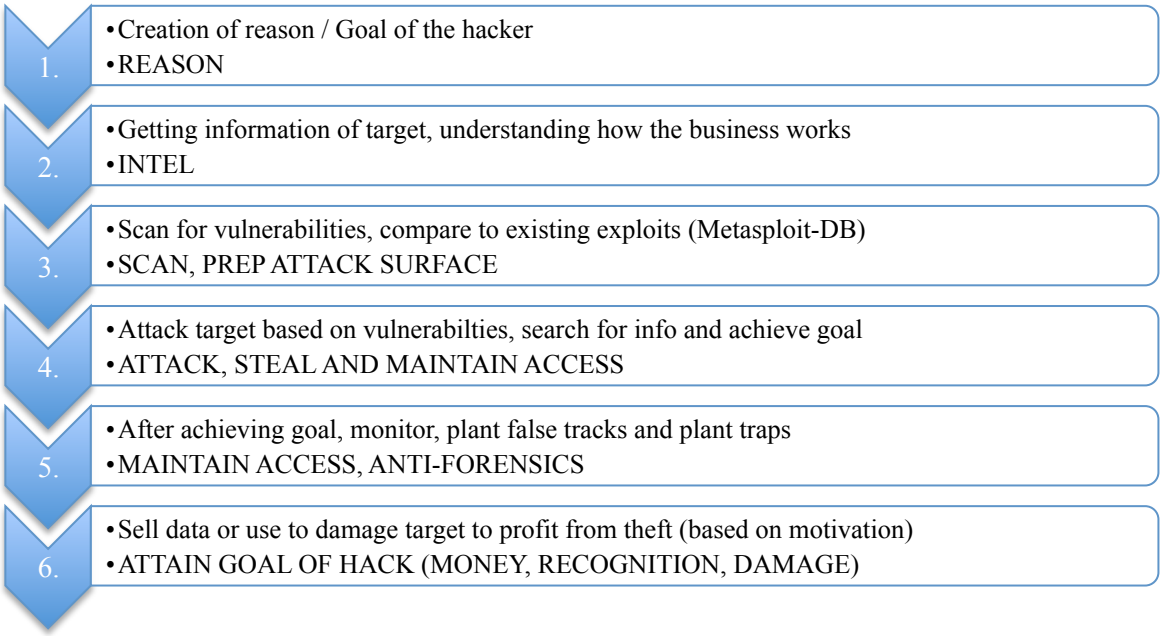


FIGURE 8: HACKING – COMMON STEPS IN AN ATTACK
SOURCE: (GOEDECKER, 2014).

In recognition of this, Goedecker also went on to explain a similar idea expressed by Weiss: layered security. He explained, "when we understand that a multiple layered security strategy must complement those processes and assets then we are able to fit the right tools and mechanisms to protect any given layer correctly" (Goedecker, 2014).

Considering each of the individual's responses, it appears that they have a similar attitude regarding the security of the water infrastructure systems: it is vulnerable to attack. Where discrepancies emerge is on the topic of risk. At this point, it appears as though Weiss and the Anonymous source agree that the systems are vulnerable, but the Anonymous source maintains the view that the risk of an attack is low, based on the grounds that there are more efficient ways of obtaining mass casualties.

PART E: SUMMARY

This chapter has analyzed some of the threats that water infrastructure systems are plagued with, and has also explored two case studies relevant to the conventional terrorist threat to water infrastructure systems. In particular, the Milwaukee case study illustrates that it may in fact be easier than expected to attack water infrastructure systems. Additionally, this also sheds light on two important factors: human fallibility and lack of effective monitoring. Although this case study is not one that clearly exemplifies any intent of malicious activity, conventional terrorism studies would likely draw attention to the ease at which this parasite got through the mechanisms that were suppose to identify it. It is here where contagion propagates and potential malevolent actors may attempt to recreate this scene at another location.

The incident at the Maroochy wastewater treatment plant is a clear example of water infrastructure infiltrated by a malevolent individual, Vitek Boden. Unlike the incident

in Milwaukee, this incident had been carried out with malicious intent, as an act of retribution. In this case, conventional terrorism studies would analyze the 'us versus them' perspective that it adheres to as a means to explain the reasons behind the incident. Boden would ultimately be viewed as an unstable individual who took matters into his own hands.

In considering each incident, it is important to take a step back and understand how conventional terrorism studies would perceive either of these. In particular, Milwaukee does not contain the typical malicious individual(s) that conventional terrorism studies acknowledge as necessary to refer to an incident as a 'terrorist attack'. In this regard, Milwaukee would likely be observed as an accident, unless it can be proven that operators of the Milwaukee water treatment plant had malicious intent.

The case of Maroochy however, would likely be the complete opposite. Given the presence of an individual with malicious intent – conventional terrorism studies would also likely argue that Boden was mentally unstable – it is much easier for this incident to be viewed as a 'terrorist attack'. This is because conventional terrorism studies asserts a very narrow scope of what defines terrorism. It is not 'us', it is 'them', and if 'they' are not on 'our' side, 'they' can only be against 'us'[36].

[36] Quite similar to George W. Bush's proclamation *you're either with us or against us* in his post 9/11 speech.

CHAPTER 5 CRITICAL TERRORISM STUDIES PERSPECTIVE ON WATER SECURITY

5.1 VIGILANCE

The case studies in the previous section have drawn attention to vulnerability, and therefore, the need to be vigilant. Often, the *possibility* of incidents occurring is associated with the *probability* of such an incident to transpire. The reality however, is possibility and probability are two terms that are independent of each other. While vigilance is required to ensure that water infrastructure systems are not attacked, there are other concerns that surround water infrastructure, such as the neglect to maintain it.

Again, perspectives on terrorism are immensely subjective. The essence of critical terrorism studies however, depicts the notion of defeating terrorism through addressing its root causes. Addressing the root causes of terrorism is undoubtedly a difficult task that will require more than just understanding moral justification, and it is in no way a short-term task. Instead it is a task that will require long-term resources and effort to understand one of the most crucial questions that critical terrorism studies attempts to answer: *why?* Why this individual? Why now? Why did he/she choose that target? Furthermore, trying to understand this through the lens of one's personal beliefs will only subvert an already subjective issue thereby creating bias, which is why the interdisciplinary nature of critical terrorism studies is significant. The end state is to decrease the frequency and severity of attacks. The interdisciplinary nature of critical terrorism studies communicates this well within its work, which is why it is employed here.

This chapter will focus on critical studies of terrorism, and will therefore consider the perspective of water infrastructure failing as a result of a number of causes, coupled

with a broader perspective of how terrorism is perceived. Additionally, it will also consider alternate forms of water infrastructure that may limit the vulnerability of the current water infrastructure systems in place.

5.2 WALKERTON

In May 2000, the town of Walkerton experienced an outbreak of a biological agent (E-coli). The outcome of this tragedy included "more than 2,300 individuals who experienced gastroenteritis, 65 who were hospitalized, 27 that had developed haemolytic uraemic syndrome (HUS; a serious and potentially fatal kidney ailment), and seven died" (Hrudey, et al, 2003, 7-14).

Similar to the Milwaukee incident, this case study is not the result of a deliberate attack, but it identified large-scale failures in the management of a water treatment plant. Instead of alerting the public health authority of the presence of e-coli in the water, distribution was switched from the well contaminated with e-coli to a well that did not have a chlorinator, but was thought to be safe (Hrudey, et al, 2003, 7-14). Moreover, this incident clearly outlines the reality that handling a contamination before it reaches the public is severely lacking.

As indicated above, the public health authority was not made aware of the presence of e-coli in the city's water. The rationale of this stems from reforms in environmental governance that had been introduced by the provincial government under Mike Harris following the election of 1995 (Prudham, 2003, 2). According to Scott Prudham, "this tragedy is an example of broad regulatory failure and the systematic production of environmental risks by neoliberal governance reforms" (Prudham, 2003, 2). Harris Ali supports this notion:

> In the case of the Walkerton municipality, such resource limitations were exacerbated because of the trickle-down effect of government imposed budget cuts to the Ministry of Environment (MOE) in 1996. Forced to work on a reduced budget, the MOE introduced certain changes related to the monitoring and oversight of drinking water supplies—changes that had significant impacts on the disaster incubation in Walkerton. First, whereas previously the MOE laboratories had conducted all routine drinking water tests for municipal water systems throughout the province, with the imposed budget restrictions, such testing was to be completed by private laboratories hired by the individual municipality. Consequently, the municipality was forced to assume the costs of this privatized testing (Ali, 2004, 2607).

Essentially, with the municipality assuming these new costs the capacity of regulatory agencies in the Ontario government were being undermined, thereby creating regulatory gaps that reckoned Walkerton a 'normal accident'[37] of neoliberalism (Prudham, 2003, 2).

In sum, the provincial government had removed itself from the responsibility of water management (quality control), and did not introduce any certification program or procedures of notification for the private labs to follow – effectively leaving the province *without* any type of "groundwater protection, management plan, or binding water quality standards" (Prudham, 2003, 9). Previously, this work had indicated that within the distribution system, there is a lack of any ability to handle a contamination before it reaches the public. The perspectives offered by Ali and Prudham hold an alternative perspective on this matter and compels one to reconsider the threats to water infrastructure. Additionally, it may even go a step further and force a dialogue on exactly what constitutes state terrorism. Analyzing this case study from such perspective essentially creates more questions than it answers. Is this a viable example of terrorism? Or does this qualify more as criminal negligence?

As discussed in the Overview of this work, Critical Terrorism Studies (CTS) addresses the role of states and government agencies in using violence against their own

[37] A term coined by Charles Perrow, 'Normal Accidents' to describe catastrophic failures in systems whose characteristics make such events inevitable (Perrow 1999; Prudham, 2003, 3).

citizens, or citizens of foreign countries (Lutz, 2010, 31). Given this, it is of use to question how the events of Walkerton may be viewed from the perspective of CTS. If not anything else, Walkerton demonstrates a great need for rethinking the maintenance of water infrastructure. There is no doubt that water infrastructure is in a deteriorating condition. In Toronto, bursting water mains have become quite a common occurrence, with an average of 1,400 water main breaks annually[38] as a result of mechanical or structural failure[39] (City of Toronto, 2014b). Bearing this, CTS may investigate the grounds on whether or not this is in fact 'state terrorism'. Certainly, terrorism is a perplexing topic in and of itself, but it is critical to note that it does not stipulate individuals being *subject to attack*. There is an array of variables to consider. Taking into context the events of Walkerton as they have been presented by the Media, and how both Ali and Prudham have presented them, one can make an informed decision, cognizant of both perspectives, on how – if at all – privatization and neoliberalization have a role in state terrorism.

As previously indicated, Walkerton demonstrates a great need for rethinking the maintenance of water infrastructure systems. Generally speaking, much of the water infrastructure system is located underground, which makes fixing any issues troublesome and expensive to say the least. One scheme that would perhaps allow for a more sustainable approach to part of the infrastructure includes sustainable stormwater management – a scheme that focuses attention on natural solutions that would "combine function and performance with environmental, economic, and social benefits" (Wang, 2014, ii). It is understood that such a scheme would include the use of 'low impact development' such as

[38] "North York, Scarborough and Etobicoke experience the highest break rates as their water mains are located in predominantly clay soil as opposed to sand" (City of Toronto, 2014b)

[39] The main factors responsible for water main deterioration and failure are: external corrosion, wall thickness, and temperature (prolonged periods of cold). For a full list, see (City of Toronto, 2014b).

green roofs, permeable surfaces[40] and planting more trees that absorb more water (Wang, 2014, 5-8). Not only would implementing a sustainable plan be beneficial to the environment, but it would also be less prone to failure and create less vulnerability for the water infrastructure system (waste) as a whole, which would moreover make the infrastructure less of an ideal target for terrorist attacks.

In her work, Wang puts forward the argument that urban areas have become dependent on engineered infrastructures (Wang, 2014, 11; Jones and Macdonald, 2007, 536). More and more, these engineered infrastructures continue to be placed under increasing demands and pressure as cities grow (Wang, 2014, 12). The sheer cost of replacing or fixing infrastructure can be quite challenging for smaller municipalities (Wang, 2014, 12), which may push some to "replace aged systems with a more integrated approach to accomplish multiple goals in water supply and waste water management while realizing cost benefits" (Donofrio et al, 2009, 180). Furthermore, this has triggered alternate forms of water management that focus on long-term sustainability, resilience, and cost efficiency: low impact development. This strategy is an "integrated water management system that encompasses low-impact design, water conservation and recycling, water quality management, and urban ecology" (Donofrio et al, 2009, 179).

This strategy seeks to utilize sustainable methods as an alternate approach to traditional water infrastructure systems that can be costly to repair. It seeks to improve water quality characteristics "by increasing retention, detention, infiltration, and treatment of stormwater runoff at its source" (Donofrio et al, 2009, 183) in opposition to directing runoff off-site as quickly as possible through both structural and non-structural means

[40] For example, "permeable or fractured bedrock may store higher volumes of water in comparison to bedrock that has minor fractures and stores small volumes of water for short periods. Depending on the connectivity of the bedrock, it may even funnel the water into subsurface storage" (Wang, 5, 2014).

(Wang, 2014, 13-16). The benefit of adopting such a strategy would not only be cost effective, but could potentially decrease the vulnerability of water infrastructure systems as a whole. However, it is important to note here, that removing a "hard target" such as the engineered systems that make up the current water infrastructure systems does not completely solve the problem of vulnerability, but instead makes the system more decentralized, which decreases the risk of an attack from occurring. Essentially, there are pros and cons to any solution that deals with critical infrastructure.

The strategy of low impact development would greatly benefit the environment, and significantly decrease risk. However, it may also transfer the responsibility of risk reduction directly to the individual. Depending how the system is implemented, the onus of water security may fall to individual households, similar to how households on well water and septic tanks are responsible for ensuring the safety of their own water. Additionally, it is also important to question if this would be a viable option to distribute and collect water to other critical infrastructures that depend on large amounts of water, as well as those industries whose waste-water contains toxic material that may disrupt the ecosystem it is a part of. Given this, it is imperative to understand that there are risks to any system that will be put in place, which is why it is crucial for each municipality to determine the level of risk it is willing to accept, and from there, to determine which system best suits its needs.

CHAPTER 6 CONCLUSION: AUTHOR'S ASSESSMENT

The majority of this work has assessed water management and the risk of terrorist attacks from a conventional terrorism studies perspective. From that perspective, this work has discussed the systems involved in the treatment of water and wastewater, and how each of the processes can be vulnerable to a biological, chemical, cyber or physical attack. Moreover, it has also shed light on how each of these threats may be realized, and has also utilized case studies and professional interviews to bring forward various perspectives, discrepancies or controversies on this subject.

As a way forward, it will be critical for water utilities to be mindful of the evolving threat landscape, especially since much of the older water infrastructure systems were not built with security as an objective (Van Leuven, 2011, 41). As it currently stands, it would appear that the current water infrastructure in Toronto remains vulnerable at a number of points, especially within the distribution system, and perhaps even the treatment facilities. However, as the individuals interviewed have suggested, the risk to water infrastructure is low at the moment. How risk is perceived is dependent on the threat factors that one is assessing. The case studies in this work have illustrated that threats can occur from a range of sources, and can be intentional or unintentional.

But in addition, using critical terrorism studies perspective, one can question ones definition of 'terrorism' suggesting that negligence to maintain and alter such infrastructure may or may not contribute to "terror". I am not alluding to a notion of 'state terror' against its own citizenry, but instead calling into question the entire definition of terrorism, and pointing to the necessity to consider a number of definitions and theories when trying to unravel this term.

Whether or not there is a legitimate threat to water infrastructure via terrorism depends on how one defines terrorism –whether from the conventional (traditional dominant) views of terrorism, or from the Critical Terrorism Studies perspective presented in this work. As such, it is essential to take precaution in analyzing what constitutes a threat, and how such a threat may be realized. Threats may not be limited to an imminent occurrence, and as such one must consider a number of scenarios and perspectives as a means of precaution, in an attempt to understand the threat environment.

Alas, it would be erroneous to state that threats are limited to biological, chemical, physical and cyber attacks. As the case studies have demonstrated, there are other matters of concern. Privatization initiatives and neoliberal reforms, such as illustrated in Walkerton, as well as a number of water main bursts in Toronto are prime examples that illustrate the need to tackle the problem in its entirety, as opposed to simply putting a 'band aid' on the issue.

Essentially, the author believes that while Toronto's current water infrastructure is clearly vulnerable, assessing its risk is quite fluid in that it may change with how critical the system is to its location, the effect the adversary wishes to achieve, and on the recognisability (public significance) of the system. To date, the recognized tool amongst critical infrastructure professionals in assessing risk is the use of the CARVER matrix. This matrix is provided below and is further explained in Appendix 6.

Score	Criticality	Accessibility	Recoverability	Vulnerability	Effect on Populace	Recognisability
5	Needed for survival	Public	Difficult	Unable to harden	Mass casualties: high symbolism	Unique
4	Needed for economic	Government or political process recognisable	Admission criteria	One year or more	Can be hardened	Deaths occur; symbolism to some
3	Disruption severe	Screening	One month to one year	Hardened for natural disasters	Injuries; symbolism important	Moderate difficulty to identify
2	Disruption moderate	Inspection of packages	One week	Hardened against snipers and attacks	Major injuries; undetermined symbolism	Very difficult to identify
1	Disruption light	Escort needed	Less than seven days	Hardened against bombs	Minor injuries; not symbolic	Indistinguishable from surroundings

FIGURE 9: CARVER MATRIX[41]
SOURCE: (BIRKETT, ET AL, 2011, 467).

Additionally, as a means to understand the range of threats that water systems may confront, employees at the utility must also recognize the types of adversaries, malevolent persons, or groups that may attempt to obstruct the utility from performing any one of its essential functions (Van Leuven, 2011, 33). This knowledge, or intelligence, would overall allow the utilities to construct a 'comprehensive threat profile' (Van Leuven, 2011, 33) as a critical factor in its risk calculation. However, the author also recognizes that the largest challenge in any circumstance is funding. Given that the number of incidents is not very high, in addition to the perceived attack immunity, putting more money toward a program that would increase the utilities' resilience to attacks may not be something we will see in the near future. Perhaps "the only trigger to change will be when, not if, an attack happens" (Sauder, 2010, 20).

[41] "The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are given a numerical value. This value represents the desirability of attacking the target. The values are then placed in a decision matrix. After CARVER values for each target or component are assigned, the sum of the values indicate the highest value target or component to be attacked" (U.S. Government, 1991, Appendix D). For additional information, please refer to Appendix 6.

Should an incident happen, whether it is accidental or intentional, a plan must be in place. Perhaps the most sensitive of issues would arise if a 'terrorist attack' on any water infrastructure system occurs. After 9/11, one of the first acts of retaliation in Canada occurred in Hamilton, where individuals set fire to a Hindu Temple (The Canadian Press, 2013). Not only did this unfortunate incident insinuate ignorance, it also drew attention to the community divide that immediately occurred soon after the attacks. As such, it is imperative that community education and outreach is available to ensure the fight and marginalization is not brought to innocent people.

The first chapter of this work brought forward two theories of terrorism: conventional (traditional) terrorism studies and critical terrorism studies. While both theories contribute to the ongoing study of terrorism, one must be mindful that terrorism is a dynamic subject, amorphous in structure. Individually, each theory will leave gaps in the ongoing study of this subject. For this reason, it is essential for both traditional and critical terrorism scholars to work together in the long term, with a view to come to grips with this thing called terrorism.

APPENDIX 1

APPENDIX 1: SELECTION OF HISTORICAL WATER THREATS AND INCIDENTS
SOURCE: ADAPTED DIRECTLY FROM (BIRKETT, ET AL, 2011, 459).

Year	Location	Incident	Description	Terrorism/other
2450–2400 BC	City of Umma, Middle East	Water diverted from adjacent state of Umma as tactical strategy by Urlama, King of Lagash	Denial of water service as political strategy	Form of terrorism to gain power over other state in lieu of warfare
600 BC	Cirrha City	Rye ergot inserted into local water supply. Cirrhaeans then became violently ill	Solon of Athens besieged Cirrha for a wrong interpretation to the Temple of Apollo. This facilitated the capture of Cirrha City	Biowarfare or bioterrorism
1748 AD	New York, USA	Angry mob burnt down a ferry house on the Brooklyn Shore of the New York East River	Revenge action for unfair allocation of water rights from the New York East River	Form of terrorism
1907–1913	Owens Valley of California, USA	Repeated dynamiting of water aqueduct system due to local concern over water being diverted to meet the needs of the growing city of Los Angeles	Farmers within the agricultural area of Owens Valley took extreme action to preserve the limited water reserves for agriculture in lieu of the city diversion	Form of terrorism taking extreme action to secure limited water supplies from being diverted from agricultural use to larger urban population
1961	Kiev, Ukraine	Dam failure subsequent to heavy rain	Babi Yar loam pulp dump dam failure led to 1,500–2,000 deaths of villagers	An unplanned event in the dam operation leading to imprisonment of senior officials
1963	Vajont Dam, North East Italy	Dam failure from overtopping	Landslide into dam caused overtopping, leading to flooding of several villages and deaths of 2,000 people	An unanticipated event due to existing geological instability on edges of dam storage
1979	Morvi Dam, Gujarat, India	Dam failure, subsequent to heavy rain and massive flooding	Machchu-2 dam failure resulting in the deaths of 1,500–15,000 villagers	Weather-induced event exceeding the design parameters of the dam
1993	Milwaukee, USA	*Cryptosporidium* water-born parasite	*Cryptosporidium* parasite commences a life cycle within the digestive tract of domestic animals such as cattle, which in this case washed into the water storages. This parasite can survive filtration and water disinfection. It caused severe illness and resulted in over 100 deaths	An unintended consequence of stock agriculture within a catchment area of water storage

APPENDIX 2

APPENDIX 2: **TORONTO WATER TREATMENT PLANT 2013 STATISTICS**
SOURCE: ADAPTED DIRECTLY FROM (CITY OF TORONTO, 2014)

R.C. HARRIS WATER TREATMENT PLANT 2013 STATISTICS

TOTAL ANNUAL PLANT WATER PRODUCED	148,380 MILLION LITRES
PERCENTAGE OF PLANT WATER PRODUCED TO THE OVERALL SYSTEM	34%
NUMBER OF DAYS THE PLANT OPERATED	349 DAYS
AVERAGE DAILY PRODUCTION	407 MILLION LITRES
MAXIMUM DAY'S PRODUCTION	689 MILLION LITRES
DATE OF MAXIMUM WATER PRODUCTION	MARCH 5, 2013

F.J. HORGAN WATER TREATMENT PLANT 2013 STATISTICS

RATED CAPACITY	800 MILLION LITRES CONVEYED PER DAY
TOTAL ANNUAL PLANT WATER PRODUCED	87,364 MILLION LITRES
PERCENTAGE OF PLANT WATER PRODUCED TO THE OVERALL SYSTEM	20%
NUMBER OF DAYS THE PLANT OPERATED	365 DAYS
AVERAGE DAILY PRODUCTION	239 MILLION LITRES/DAY
MAXIMUM DAY'S PRODUCTION	483 MILLION LITRES
DATE OF MAXIMUM WATER PRODUCTION	DECEMBER 2, 2013

R.L. CLARK WATER TREATMENT PLANT 2013 STATISTICS

TOTAL ANNUAL PLANT WATER PRODUCED	115,015 MILLION LITRES
PERCENTAGE OF PLANT WATER PRODUCED TO THE OVERALL SYSTEM	26%
NUMBER OF DAYS THE PLANT OPERATED	348 DAYS
AVERAGE DAILY PRODUCTION	328 MILLION LITRES
MAXIMUM DAY'S PRODUCTION	473 MILLION LITRES
DATE OF MAXIMUM WATER PRODUCTION	JULY 19, 2013

ISLAND WATER TREATMENT PLANT 2013 STATISTICS

TOTAL ANNUAL PLANT WATER PRODUCED	87,947 MILLION LITRES
PERCENTAGE OF PLANT WATER PRODUCED TO THE OVERALL SYSTEM	20%
NUMBER OF DAYS THE PLANT OPERATED	341 DAYS
AVERAGE DAILY PRODUCTION	254 MILLION LITRES
MAXIMUM DAY'S PRODUCTION	354 MILLION LITRES
DATE OF MAXIMUM WATER PRODUCTION	JULY 18, 2013

APPENDIX 3

COMPOUNDS OF CONCERN FOR DRINKING WATER SECURITY
SOURCE: ADAPTED DIRECTLY FROM (KROLL, 2013, 8-9)

HEAVY METALS: Heavy metals are agents of concern due to their toxicity to humans. They are also fairly easy to obtain, and their salts tend to be readily soluble

HERBICIDES: While as a general class, herbicides tend to be less detrimental to human health than some other compounds; there are some notable exceptions. This, along with the ability to easily obtain large quantities of these chemicals from agricultural supply sources, adds to the concern. Even if few fatalities resulted, the panic caused by the introduction of herbicide type compounds into a water system could be severe.

INSECTICIDES: Insecticides tend to be more harmful to human health than herbicides. Some of the insecticides have chemical structures quite similar to some of the chemical warfare nerve agents, and there are several that are cholinesterase inhibitors. Like herbicides, insecticides are also readily available in large quantities. For some, their solubility limits their usefulness as water introduced weapons, but others are quite soluble and present more of a threat.

NEMATOCIDES AND RODENTICIDES: Nematocides are similar to insecticides. They, with some exceptions, do tend to be more soluble than insecticides. Some nematocide compounds are also similar to chemical warfare agents in structure and mode of action. Rodenticides are of concern because they are specifically designed to be lethal to mammalian species such as humans. Both classes are readily available in large quantities.

INDUSTRIAL CHEMICALS AND MISCELLANEOUS AGENTS: There are any number of industrial chemicals that could be used in an attack. Chief among these is cyanide, which is widely used in mining and other industries.

ILLEGAL DRUGS: Illegal drugs are not widely recognized as a potential threat. Street drugs, such as LSD, GHB, PCP and heroin, among others, are a mode of attack that could be employed. Some drugs, such as LSD, are easily synthesized in a home lab. Other drugs, such as heroin, are widely available. While the cost could be prohibitive for individuals working alone, supplies do exist for well-organized and funded groups. Also, it should be noted that a large portion of the illegal opiates (such as heroin) finding their way into the US come from areas such as West Asia where the terrorist cells often control this trade.

RADIONUCLIDES: The use of radionuclides as a terror weapon is a distinct possibility. Even if casualties were low, the psychological impact of a radiological threat could be severe. Obtaining high purity, highly radioactive material, such as plutonium or Uranium 238, is difficult, and it is unlikely that a terrorist organization that had obtained these materials would be inclined to use them in an attack on a water system. More likely is the use of low level radioactive material or waste

COMMERCIAL PRODUCTS: While not the weapons of choice for organized terrorists, lone saboteurs, the emotionally unstable or small groups may turn to easily obtained commercial products such as bug sprays or lawn chemicals. Many of the active ingredients of these preparations are the same as the pesticides and herbicides already discussed. The difference lies in the smaller proportion of active ingredients. The vast majority of these compounds have inert ingredients listed as their main component.

CHEMICAL WARFARE AGENTS: Chemical warfare agents such as VX, Soman, and Sarin along with older type chemical weapons such as Mustard Gas and Lewisite are not likely to be targeted against a water system due to their limited availability. If they are used, it is more likely that any assault from these weapons will be via aerosol. As the result of an aerosol attack it is possible and even likely that these agents could find their way into water supplies.

TOXINS AND BIOAGENTS: There are a number of protozoa, bacteria, viruses and toxins that could be utilized in an attack. Many of these materials are extremely toxic with compounds such as botulinum toxin being some of the most toxic substances known. These types of materials are fairly easy to grow or extract from readily available sources. For example ricin is extracted from castor beans and abrin can be obtained form rosary peas. There are several examples of the elicit production of ricin by terrorists. Bacteria can also be easily grown. For an attack on water the production of these materials may be even simpler than for an aerosol attack as there is little need to modify the toxins to make them airborne. In fact even raw sewage could be used as a potential contaminant in a backflow or cross connection type attack.

APPENDIX 4

SCADA VULNERABILITIES

ADOPTED DIRECTLY FROM (FABRO, 2012, 46-47).

Vulnerabilities and SCADA System Availability

To facilitate the alignment of vulnerabilities with threat and consequence, the study team determined that the common denial of service vulnerabilities resulted from:
-Improper bounds checking for data inputs, resulting in buffer overflows that can be used to write into random or specific memory space
-Improper session management leading to a uncontrollable unmanaged connection states -Factory deployed emergency shutdown capability, allowing for shutdown or reboot once an undocumented password is used
-Default reboot protocol, allowing an attacker to force system reboots ad infinitum -Memory leaks on physical devices creating opportunities for extensive resource consumption -Embedded diagnostic utilities that can create resource consumption failures when activated during normal system operation (on-line)
-Heap buffer overflows resulting in denial of service when excessively long data strings are submitted following valid packet streams
-Unauthorized access to embedded device Web servers allowing for an adversary to set refresh rates so high it renders the user interface inoperable
-Critical devices vulnerable to loading and executing corrupted firmware, resulting in a system malfunction and denial of service
-Inappropriately programmed field equipment forced into sending bulk multicast network subscription messaging, thus flooding the network and preventing normal control communications
-Various buffer overflow vulnerabilities resulting in the corruption (and non-functioning) of embedded device web pages and remote connection services (ftp, telnet, rsh etc) -Various instances of NULL pointer dereferencing
-Denial of service due to performance failures from service scans and enumeration, some resulting in system auto-restore to factory settings (and thus being rendered unusable in a production environment)

Vulnerabilities and SCADA System Integrity

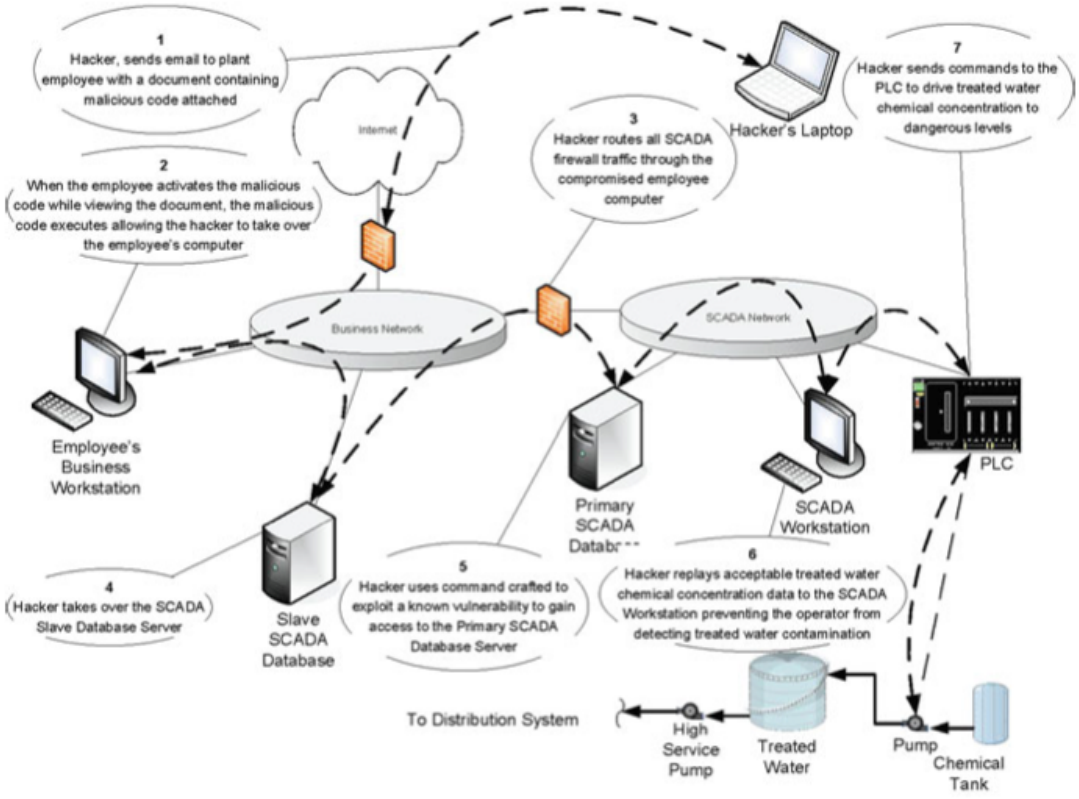
To facilitate realignment of vulnerabilities with threat and consequence, the study team determined that the common integrity vulnerabilities resulted from:
-Improper bounds checking for data inputs, resulting in buffer overflows that can be used to write into random or specific memory space and resulted in the creation of new users or the execution of arbitrary code
-Hard-coded and/or known default passwords used for system administration -Inappropriate use of least privilege practices, allowing an attacker to exploit one system application to gain access into more authoritative ones
-Embedded web services vulnerable to cross site scripting
-Unrestricted file content uploads and no destination bounds checking
-Various database and SQL injection vulnerabilities resulting in modification of operational data or creation unauthorized (but privileged) users

-Critical devices vulnerable to loading and executing modified firmware (with the intent to create new user accounts or remove credential requirements)
-Lack of message authentication facilitating for various man-in-the-middle type of attacks -Various buffers overflow vulnerabilities resulting in the modification of embedded device web pages and authorized host listings

Vulnerabilities and SCADA System Confidentiality

To facilitate realignment of vulnerabilities with threat and consequence, the study team determined that the common confidentiality vulnerabilities resulted from:
-Plaintext communications between operator control environments and field devices, allowing for the extraction of credentials
-Poor password obfuscation and client-side storage of authentication credentials -Unsecured directory traversal vulnerabilities
-Unauthenticated acquisition of user and system configurations direct from field devices and operator consoles

APPENDIX 5



APPENDIX 5: SCADA NETWORK ATTACK SCENARIO
SOURCE: ADAPTED FROM (ELLIS, ET AL, 2011, 295).

APPENDIX 6

6.1 CARVER MATRIX: The CARVER Matrix is a tool that can be utilized to determine which identified targets will have the 'biggest payoff' to the overall mission.

Score	Criticality	Accessibility	Recoverability	Vulnerability	Effect on Populace	Recognisability
5	Needed for survival	Public	Difficult	Unable to harden	Mass casualties: high symbolism	Unique
4	Needed for economic	Government or political process recognisable	Admission criteria	One year or more	Can be hardened	Deaths occur; symbolism to some
3	Disruption severe	Screening	One month to one year	Hardened for natural disasters	Injuries; symbolism important	Moderate difficulty to identify
2	Disruption moderate	Inspection of packages	One week	Hardened against snipers and attacks	Major injuries; undetermined symbolism	Very difficult to identify
1	Disruption light	Escort needed	Less than seven days	Hardened against bombs	Minor injuries; not symbolic	Indistinguishable from surroundings

SOURCE: ADAPTED DIRECTLY FROM (BIRKETT, ET AL, 2011, 467).

"The CARVER factors and their assigned values are used to construct a CARVER matrix. This is a tool for rating the desirability of potential targets and wisely allocating attack resources…To construct the matrix, list the potential targets in the left column. The Table below shoes a sample matrix for a bulk electric power supply facility" (U.S. ARMY, 1991, APPENDIX D).

APPENDIX 6.2: COMPLETED CARVER MATRIX

BULK ELECTRIC POWER SUPPLY							
POTENTIAL TARGETS	C	A	R	V	E	R	TOTAL
FUEL TANKS	8	9	3	8	5	6	41
FUEL PUMPS	8	6	2	10	5	3	34
BOILERS	6	2	10	4	5	4	31
TURBINES	8	6	10	7	5	9	45
GENERATORS	4	6	10	7	5	9	41
CONDENSERS	8	8	5	2	5	4	34
FEED PUMPS	3	8	5	8	5	6	33
CIR. WATER PUMPS	3	6	5	8	5	4	33
GENERATOR STEP UP TRANSFORMER	10	10	10	9	5	9	53

SOURCE: ADAPTED DIRECTLY FROM (U.S. ARMY, 1991, APPENDIX D).

APPENDIX 6.3: ASSIGNING VALUES TO THE CARVER MATRIX

SOURCE: ADAPTED DIRECTLY FROM (U.S. ARMY, 1991, APPENDIX D).

ASSIGNING CRITICALITY VALUES

CRITERIA	SCALE
Immediate halt in output, production, or service; target cannot function without it	9-10
Halt within 1 day, or 66% curtailment in output, production, or service	7-8
Halt within 1 week, or 33% curtailment in output, production, or service	5-6
Halt within 10 days, or 10% curtailment in output, production, or service	3-4
No significant effect on output, production, or service	1-2

ASSIGNING ACCESSIBILITY VALUES

CRITERIA	SCALE
Easily accessible, standoff weapons can be employed	9-10
Inside a perimeter fence but outdoors	7-8
Inside a building but on ground floor	5-6
Inside a building but on second floor or in basement; climbing or lowering required	3-4
Not accessible or inaccessible without extreme difficulty	1-2

ASSIGNING RECUPERABILITY VALUES

CRITERIA	SCALE
Replacement, repair, or substitution requires 1 month or more	9-10
Replacement, repair, or substitution requires 1 week to 1 month	7-8
Replacement, repair, or substitution requires 72 hours to 1 week	5-6
Replacement, repair, or substitution requires 24 to 72 hours	3-4
Same day replacement, repair, or substitution	1-2

ASSIGNING VULNERABILITY VALUES

CRITERIA	SCALE
Vulnerable to long-range laser target designation, small arms fire, or charges of 5 pounds or less	9-10
Vulnerable to light antiarmor weapons fire or charges of 5 to 10 pounds	7-8
Vulnerable to medium antiarmor weapons fire, bulk charges of 10 to 30 pounds, or very careful placement of smaller charges	5-6
Vulnerable to heavy antiarmor fire, bulk charges of 30 to 50 pounds, or requires special weapons	3-4
Invulnerable to all but the most extreme targeting measures	1-2

ASSIGNING EFFECT VALUES

CRITERIA	SCALE
Overwhelmingly positive effects; no significant negative effects	9-10
Moderately positive effects; few significant negative effects	7-8
No significant effects; neutral	5-6
Moderately negative effects; few significant positive effects	3-4
Overwhelmingly negative effects; no significant positive effects	1-2

ASSIGNING RECOGNIZABILITY VALUES

CRITERIA	SCALE
The target is clearly recognizable under all conditions and from a distance; it requires little or no training for recognition 3-4	9-10
The target is easily recognizable at small-arms range and requires a small amount of training for recognition	7-8
The target is difficult to recognize at night or in bad weather, or might be confused with other targets or target components; it requires some training for recognition	5-6
The target is difficult to recognize at night or in bad weather, even within small-arms range; it is easily confused with other targets or components, it requires extensive training for recognition	3-4
The target cannot be recognized under any conditions, except by experts	1 -2

"As each potential target is evaluated for each CARVER factor, enter the appropriate value into the matrix. Once all the potential targets have been evaluated, add the values for each potential target. . The sums represent the relative desirability of each potential target; this constitutes a prioritized list of targets" (U.S. ARMY, 1991, APPENDIX D).

APPENDIX 7

PERSPECTIVES ON SECURITY
SOURCE: (DHS, 2009, 5)

SECURITY TOPIC	INFORMATION TECHNOLOGY (IT)	CONTROL SYSTEMS (ICS)
ANTIVIRUS AND MOBILE CODE	VERY COMMON; EASILY DEPLOYED AND UPDATED	CAN BE VERY DIFFICLT DUE TO IMPACT ON ICS; LEGACY SYSTEMS CANNOT BE FIXED
PATCH MANAGEMENT	EASILY DEFINED; ENTERPRISE WIDE REMOTE AN AUTOMATED	VERY LONG RUNWAY TO SUCCESSFUL PATCH INSTALL; OEM SPECIFICL MAY IMPACT PERFORMANCE
TECHNOLOGY SUPPORT LIFETIME (OUTSOURCING)	203 YEARS; MULTIPLE VEDORS; UBIQUITOUS UPGRADES	10-20 YEARS; SAME VENDOR
CYBER SECURITY TESTING AND AUDIT (METHODS)	USE MODERN METHODS	TESTING HAS TO BE TUNED TO SYSTEM; MODERN METHODS INAPPROPRIATE FOR ICS; FRAGILE EQUIPMENT BREAKS
CHANGE MANAGEMENT	REGULAR AND SCHEDULED; ALIGNED WITH MINIMUM-USE PERIODS	STRATEGIC SCHEDULING; NON TRIVIAL PROCESS DUE TO IMPACT
ASSET CLASSIFICATION	COMMON PRACTICE AND DONE ANNUALLY; RESULTS DRIVE CYBER SECURITY EXPENDITURE	ONLY PERFORMED WHEN OBLIGATED; CRITICAL ASSET PROTECTION ASSOCIATED WITH BUDGET COSTS
INCIDENT RESPONSE AND FORENSICE	EASILY DEVELOPED AND DEPLOYED; SOME REGULATORY REQUIREMENTS; EMBEDDED IN TECHNOLOGY	UNCOMMON BEYOND SYSTEM RESUMPTION ACTIVITIES; NO FORENSICS BEYOND EVENT RE-CREATION
PHYSICAL AND ENVIRONMENTAL SECURITY	POOR (OFFICE SYSTEMS) TO EXCELLENT (CRITICAL OPERATIONS SYSTEMS)	EXCELLENT (OPERATIONS CENTERS; GUARDS, GATES, GUNS)
SECURE SYSTEMS DEVELOPMENT	INTEGRAL PART OF DEVELOPMENT PROCESS	USUALLY NOT AN INTEGRAL PART OF SYSTEMS DEVELOPMENT
SECURITY COMPLIANCE	LIMITED REGULATORY OVERSIGHT	SPECIFIC REGULATORY GUIDANCE (SOME SECTORS)

APPENDIX 8

PRIORITIES OF SECURITY

SOURCE: (DHS, 2009, 5)

SECURITY PRIORITIZATION FOR IT PROFESSIONALS

CONFIDENTIALITY	HIGH IMPORTANCE
INTEGRITY	HIGH IMPORTANCE
AVAILABILITY	LOWER IMPORTANCE

SECURITY PRIORITIZATION FOR ICS OPERATORS

AVAILABILITY	VERY HIGH IMPORTANCE
INTEGRITY	MEDIUM IMPORTANCE
CONFIDENTIALITY	LOW IMPORTANCE

WORKS CITED

Abrams, Marshall D. and Joe Weiss. (2008). Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia. MITRE Corporation. March 2014. Available from <http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_briefing.pdf>.

Ahmadi Azadeh, Mohammad Karamouz F., and Sara Saadati. (2010). Vulnerability Assessment and Risk Reduction of Water Supply Systems. World Environmental and Water Resources Congress 2010. March 2014. Available from <https://www.academia.edu/548158/Vulnerability_Assessment_and_Risk_Reduction_of_Water_Supply_Systems>.

Ali, S.H. (2004). A Socio-ecological Autopsy of the E. Coli 0157:H7 Outbreak in Walkerton, Ontario, Canada. Social Science & Medicine. 58: 2601-2612. April 2014. Available from <http://tusk.tufts.edu/auth/pdf/555017.pdf>.

Alibaba. (2014). Sodium Cyanide for Purchase. March 2014. Available from <http://www.alibaba.com/showroom/sodium-cyanide.html?uptime=20121129&ptsid=1013000015669012&crea=28367223020&plac=&netw=g&device=c&ptscode=0110202060010001>.

Alibek, Ken. (1999). Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told From Inside by the Man Who Ran It. New York:Delta Trade Paperbacks.

Anonymous. (2014). Email Interview. March 2014.

Bahadur, R. and William B. Samuels. (2011). Water/Wastewater Infrastructure Security: Threats and Vulnerabilities. *Handbook of Water and Wastewater Systems Protection.* R.M. Clark et al. (Eds). Washington DC: Springer Science + Business Media. Pp. 65-85.

BBC. (2014). Deadly Plague and Botulism Microbe Found in US Lab. BBC News. September 2014. Available from <http://www.bbc.com/news/world-us-canada-29089867>.

Behm, Don. (2013). Milwaukee Marks 20 Years Since Cryptosporidium Outbreak. *Journal Sentinel.* November 2014. Available from <http://www.jsonline.com/news/milwaukee/milwaukee-marks-20-years-since-cryptosporidium-outbreak-099dio5-201783191.html>.

Birkett, D., Jim Truscott, Helena Mala-Jetmarova, and Andrew Barton. (2011). Water/Wastewater Infrastructure Security: Threats and Vulnerabilities. *Handbook of Water and Wastewater Systems Protection.* R.M Clark et al. (Eds). Washington DC: Springer Science + Business Media. Pp. 457-483.

Booth, K. (2008) The Human Faces of Terror: Reflections in a Cracked Looking Glass. *Critical Studies on Terrorism.* Pp65-79.

Canadian Press, The. (2013). 3 Charged in Hindu Temple Arson in Hamilton. York Region. October 2014. Available from <http://www.yorkregion.com/news-story/4238553-3-charged-in-hindu-temple-arson-in-hamilton/>.

Chalecki, Elizabeth L. (2001) *A New Vigilance: Identifying and Reducing the Risks of Environmental Terrorism*. Oakland: Pacific Institute.

Chaney, Mike. (2012). *DHS: State of Control Systems Cyber Security.* Department of Homeland Security. Control Systems Security Workshop. Hyatt Hotel. Toronto, Ontario. 19 Nov. 2012.

Chatfield, Tom (2012). Cyber Warfare: Fear of System Failure. BBC News. October 2014. Available from <http://www.bbc.com/future/story/20120608-system-failure-in-cyber-warfare>.

City of Toronto. (2010). Toronto Water. February 2014. Available from <http://www.toronto.ca/water/>.

City of Toronto. (2014).Water Treatment. February 2014. Available from: <http://www1.toronto.ca/wps/portal/contentonly?vgnextoid=6d1409f8e0c7f310VgnVCM10000071d60f89RCRD&vgnextfmt=default>.

City of Toronto. (2014b). Watermain Breaks. April 2014. Available from: <http://www1.toronto.ca/wps/portal/contentonly?vgnextoid=9532aa55ee66f310VgnVCM10000071d60f89RCRD&vgnextchannel=6534aa55ee66f310VgnVCM10000071d60f89RCRD>.

Combs, Cindy C. (2011). *Terrorism in the Twenty-First Century*. 6th Ed. Toronto: Longman.

Conklin, William Arthur. (2011). Control Systems Personnel are from Mars; IT Personnel are from Venus. *International Journal of Critical Infrastructure Protection*. 4 (2011) 76-77. SciVerse Science Direct. Accessed Nov. 2014.

Copeland, C., M. Williams, and V. Stamper. (2012). Poisoning the Great Lakes: Mercury Emissions from Coal-Fired Power Plants in the Great Lakes Region.Natural Resources Defense Council. March 2014. Available from <http://www.nrdc.org/air/files/poisoning-the-great-lakes.pdf>.

Cornell University Law School. (2014). Actus Reus. Legal Information Institute. March 2014. Available from <http://www.law.cornell.edu/wex/actus_reus>.

Corso, P. S., M. H. Kramer, K. A. Blair, D. G. Addiss, J. P. Davis, and A. C. Haddix. (2003). Cost of Illness in the 1993 Waterborne Cryptosporidium Outbreak, Milwaukee, Wisconsin. *Emerging Infectious Diseases* 9 (4): 426-31.

Deininger, R. A. (2000). The Threat of Chemical and Biological Agents to Public Water Supply Systems. McLean, VA: Science Applications International Corporation.

DHS. (2007). Water: Critical Infrastructure and Key Resources; Sector-Specific Plan as Input to the National Infrastructure Protection Plan. Dept. of Homeland Security, February 2014. Available from <http://www.dhs.gov/ xlibrary/assets/nipp- ssp-water.pdf >.

DHS. (2009). Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Control Systems Security Program. National Cyber Security Division. Accessed Nov. 2014 from: <https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf>.

DHS. (2014). What is Security and Resilience? Dept. of Homeland Security. April 2014. Available from <http://www.dhs.gov/what-security-and-resilience>.

Dinnis, Heather Harrison. (2012). *Cyber Warfare and the Laws of War*. New York: Cambridge University Press.

Donofrio, J., Kuhn, Y., McWalter, K. and M. Winsor. (2009). Water-sensitive Urban Design: An Emerging Model in Sustainable Design and Comprehensive Water-Cycle Management. *Environmental Practice.* (11): 179-189.

Ellis, P., S. Panguluri, and W. Phillips. (2011). Cyber Security: Protecting Water and Wastewater Infrastructure. *Handbook of Water and Wastewater Systems Protection.* R.M. Clark et al. (Eds). Washington DC: Springer Science + Business Media.

Emergency Management Ontario. (2011). Glossary of Terms. October 2014. Available from <https://www.emergencymanagementontario.ca/english/emcommunity/response_resources/GlossaryOfTerms/glossary_of_terms.html>.

(EMO) Emergency Management Ontario. (2009). Progress Report 2006-2009. October 2014. Available from <https://www.emergencymanagementontario.ca/stellent/groups/public/@mcscs/@www/@emo/documents/abstract/emo_progressreport_pdf.pdf>.

Fabro, Marc. (2012). *Study on Cyber Security and Threat Evaluation in SCADA Systems*. Defence R&D Canada. DRDC CSS CR 2012-006.

Frey, Bruno S. (2004). *Dealing with Terrorism – Stick or Carrot?* Cheltenham: Edward Elgar Publishing Limited.

Frischknecht, Friedrich. (2008). The History of Biological Warfare. *Decontamination of Warfare Agents.* Andre Richardt and Marc-Michael Blum (Ed). Weinheim: WILEY-VCH Verlag GmbH & Co KGaA.

Gendron, Angela and Martin Rudner. (2012). Assessing Cyber Threats to Canadian Infrastructure. Report Prepared for the Canadian Security Intelligence Service. February 2014. Available from: <https://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp>.

Giroux, Henry A. (2005) The Terror of Neoliberalism: Rethinking the Significance of Cultural Politics. *College Literature*. (32) No. 1. November 2014. Available form <http://muse.jhu.edu/journals/lit/summary/v032/32.1giroux.html>.

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

Gleick, Peter H., Heather Cooley, David Katz, Emily Lee, Jason Morrison, Meena Palaniappan, Andrea Samulon, and Gary H. Wolff. (2007). *The World's Water 2006-2007: The Biennial Report on Freshwater Resources.* Washington: Island Press.

Goedeker, Michael. (2014). HAKDEFNET. March 2014. Available from <http://www.hakdefnet.org/H%40KDEFNET/Prereq_Info.html>.

Golden, Kate. (2013). 20 years After Fatal Outbreak, Milwaukee Leads on Water Testing. Wisconsin Center for Investigative Journalism. March 2014. Available from <http://www.wisconsinwatch.org/2013/05/22/20-years-after-fatal-outbreak-milwaukee-leads-on-water-testing/>.

Gradus, MS, A. Singh, and GV Sedmak. (1994). The Milwaukee Cryptosporidium Outbreak: Its Impact on Drinking Water Standards, Laboratory Diagnosis, and Public Health Surveillance. *Clinical Microbiology Newsletter* (8) No. 16: 57-60.

Haestad, M., Walski, T. M., Chase, D. V., Savic, D. A., Grayman, W., Backwith, S., Koelle, E. (2003). *Advanced Water Distribution Modeling and Management*. Waterbury, CT USA: Haestad Press.

Harada, M., M. Hanada, M. Tajiri, Y. Inoue, N. Hotta, T. Fujino, S. Takaoka, and K. Ueda. (2011). Mercury Pollution in First Nations Groups in Ontario, Canada: 35 years of Canadian Minamata Disease. Journal of Minamata Studies 3: 3-30. March 2014. (English Translation) Available from <http://freegrassy.net/wp-content/uploads/2012/06/Harada-et-al-2011-English.pdf>.

Hickman, D. C. (1999). A Chemical and Biological Warfare Threat: USAF Water Systems at Risk. March 2014. Available from <http://www.au.af.mil/au/awc/awcgate/cpc-pubs/hickman.htm>.

Hildick-Smith, Andrew. (2005). Security for Critical Infrastructure SCADA Systems. SANS Institute. February 2014. Available from <https://www.sans.org/reading-room/whitepapers/warfare/security-critical-infrastructure-scada-systems-1644>.

Hoover, J. E. (1941). Water Supply Facilities and National Defense. *Journal of the American Water Works Association* (33) No. 11: 861–1865.

Hrudey, SE, P. Payment, PM Huck, RW Gillham, and EJ Hrudey. (2003). A Fatal Waterborne Disease Epidemic in Walkerton, Ontario: Comparison with other Waterborne Outbreaks in the Developed World. *Water Science & Technology* (3) No. 47: 7-14.

Human Rights Voices. (2014). There is no UN Definition of Terrorism. April 2014. Available from <http://www.humanrightsvoices.org/EYEontheUN/un_101/facts/?p=61>.

IBM. (2014). The Internet of Things. October 2014. Available from <http://www-01.ibm.com/software/info/internet-of-things/>.

Infectious Disease News. (2007). Cryptosporidium in Milwaukees Water Supply Caused Widespread Illness. March 2014. Available from <http://www.healio.com/infectious-disease/gastrointestinal-infections/news/print/infectious-disease-news/%7Bc89c35b9-b521-43e5-960c-1d3809f77482%7D/cryptosporidium-in-milwaukees-water-supply-caused-widespread-illness>.

Jackson, Richard. (2008). Why We Need Critical Terrorism Studies. *E-International Relations.* September 2014. Available from <http://www.e-ir.info/2008/04/08/why-we-need-critical-terrorism-studies/>.

Jackson, Richard. (2009). Critical Terrorism Studies: An Explanation, a Defence and a Way Forward. *British International Studies Association*. April 2014. Available from <http://www.bisa.ac.uk/index.php?option=com_bisa&task=download_paper&no_html=1&passed_paper_id=54>.

Jones, P. and N. Macdonald. (2007). Making space for unruly water: Sustainable drainage systems and the disciplining of surface runoff. *Geoforum. (*38) 534-544.

Kaplan, Jeremy. (2011). Anonymous Hackers Release Stuxnet Worm Online. Fox News. March 2014. Available from <http://www.foxnews.com/tech/2011/02/15/anonymous-hackers-offer-stuxnet-worm-online/>.

Katen, K. (2004). Best Practices for Government to Enhance the Security of National Critical Infrastructure. National Infrastructure Advisory Council. March 2014. Available from <https://www.dhs.gov/xlibrary/assets/niac/NIAC_BestPracticesSecurityInfrastructures_0404.pdf>.

Kroll, Dan J. (2013). The Terrorist Threat to Water and Technology's Role in Safeguarding Supplies. Federation of Scientists. March 2014. Available from <http://www.federationofscientists.org/PlanetaryEmergencies/Seminars/45th/Kroll%20publication.docx>.

Kumar, Mohit. (2014). AirHopper – Hacking Into an Isolated Computer Using FM Radio Signals. The Hacker News. November 2014. Available from <http://thehackernews.com/2014/10/airhopper-hacking-into-isolated.html>.

Lutz, James M. (2010). A Critical View of Critical Terrorism Studies. *Perspectives on Terrorism* (4) No. 6: 31-40. April 2014. Available from <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/130>.

MacKenzie, W. R., W. L. Schell, K. A. Blair, D. G. Addiss, D. E. Peterson, N. J. Hoxie, J. J. Kazmierczak, and J. P. Davis. (1995). Massive Outbreak of Waterborne Cryptosporidium iIfection in Milwaukee, Wisconsin: Recurrence of Illness and Risk of Secondary Transmission. *Clinical Infectious Diseases* (1) No. 21: 57-62.

Maniscalchi, Jago. (2009). Threat vs. Vulnerability vs. Risk. Digitial Threat: Vulnerabilities; Exploitation; Malware; Risk; Mitigation. March 2014. Available from <http://www.digitalthreat.net/2009/06/threat-vs-vulnerability-vs-risk/>.

Merriam-Webster. (2014). Online Dictionary. April 2014. Available from <http://www.merriam-webster.com/dictionary/>.

Meisels, Tamar. (2008). *The Trouble with Terror: Liberty, Security, and the Response to Terrorism.* Cambridge: Cambridge University Press.

Perkel, C. N. (2002). *Well of Lies: The Walkerton WaterTtragedy*. Toronto: McClelland & Stewart Ltd.

Perrow, C. (1999). *Normal Accidents: Living with High-risk Technologies.* Princeton University Press, Princeton, NJ.

Poulsen, Kevin. (2002). FBI Issues Water Supply Cyberterror Warning. *Security Focus.* April 2014. Available from <http://www.securityfocus.com/news/319>.

Prudham, Scott. (2003). Poisoning the Well: Neoliberalism and the Contamination of Municipal Water in Walkerton, Ontario. *Geoforum.* April 2014. Available from <http://geography.utoronto.ca/wp-content/uploads/2013/10/Poisoningthewellproofs.pdf>.

(PSC) Public Safety Canada. (2014). Critical Infrastructure. Government of Canada. March 2014. Available from <http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx>.

(PSC) Public Safety Canada. (2014b). Currently Listed Entities. Government of Canada. April 2014. Available from <http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx>.

Sauder, Stephen. (2010). Unquenched Thirst. Sanitation Worldwide. March 2014. Available from <http://www.sanitationworldwide.com/files/5813/2147/6135/Water_Threats.pdf>.

Shea, D. A., and Library of Congress Washington DC Congressional Research Service. (2004). Critical Infrastructure: Control Systems and the Terrorist Threat. March 2014. Available from <https://www.fas.org/sgp/**crs**/homesec/RL31534.pdf>.

Simon, J. D. (1997). Biological terrorism. *JAMA* (5) No. 278: 428-30. March 2014. Available from <www.ncbi.nlm.nih.gov/pubmed/924433>.

Taleb, NAssim Nicholas. (2010). *The Black Swan*. New York: Random House Trade Paperback.

U.S. Government. (1991). FM-34-36: *Special Operations Forces Intelligence and Electronic Warfare Operations. Headquarters Department of the Army*. Washington, DC. April 2014. Available from <http://www.fas.org/irp/doddir/army/fm34-36/toc.htm>.

Van Leuven, Laurie J. (2011). Water/Wastewater Infrastructure Security: Threats and Vulnerabilities. *Handbook of Water and Wastewater Systems Protection.* R.M Clark et al. (Eds). Washington DC: Springer Science + Business Media.

Wang, Jennifer. (2014). *Beyond the Pipes: Planning for Sustainable Stormwater Management in Toronto*. Toronto: York University.

Wardlaw, Grant. (1990). *Political Terrorism: Theories, Tactics, and Counter-Measures.* 2nd ed. Cambridge: Cambridge University Press.

Weiss, Joseph. (2014). Phone Interview. March 2014.

Weiss, Joseph. (2010). *Protecting Industrial Control Systems from Electronic Threats*. New York: Momentum Press.