Water & terrorism
Using Dutch water systems as a target

Robert-Jan G. Ruifrok

Water and terrorism

Using Dutch water systems as a target

Radboud University Nijmegen

Student author: RJ. G. Ruifrok

Student number: s4264770

Course: Bachelor thesis Human Geography

Course coordinator: Drs. H. Donkers

Educational institute: Radboud University Nijmegen

                        Faculty of Management Sciences

                        (pre-master) Centre for International Conflict- Analysis & Management

Date: Friday the 16th of August 2013, Nijmegen, the Netherlands

Preface

The bachelor thesis laying in front of you has been created at the Radboud University in Nijmegen (the Netherlands) at the department of Human Geography and the Centre for International Conflict- Analysis & Management. This bachelor thesis is part of a pre-master program required for admittance to the master 'Conflicts, Territories and Identities'.

When I addressed the examination committee at the start of this academic year to apply to the pre-master, I was convinced that a master in Human Geography would positively contribute to the bachelor degree which I had obtained in Garden- & Landscape Architecture. However, at that time I had difficulty finding the direct relation, especially in finding compelling arguments to link architecture and urban planning to Human Geography. Nevertheless, after one year of different subjects and finishing with the pre-master via a bachelor thesis, many arguments can now be made. The spatial and social analysis in which I specialised during my final thesis for Garden- & Landscape Architecture helped me to connect the two studies together.

After a year of different courses such as 'Borders and Identities in Europe' and 'Conflict on the Balkan' both spatial and social analyses were made and I was sure that I had made the right decision.

That is why I wanted to create a research plan that would also integrate the spatial and social side of Human Geography. Together with the options I could choose from I decided to apply to a subject coordinated by Henk Donkers, being international water conflicts. After reading some of the recommended literature, an article from Peter Gleick written in 2006 especially caught my eye. Together with the heightening of the Dutch National Threat level for terrorism a subject was born: the relationship between water and terrorism in the Netherlands.

I would like to thank the different people who helped me with this thesis starting with Henk Donkers. Henk helped me to create a better academic view coming from a more practical study. His patience and often repeating advice has shown me the way forward. Without his calmness combined with his perseverance I would not have achieved what is now laying in front of you.

I would also like to thank my father for his second opinion on academic writing in the English language. His chemical background does not have a lot of common ground with Human Geography at first, but the subject was quickly familiar and created good late-night discussions and new insights.

Last but not least I would like to thank my brother for giving a more modern insight in academic writing and showing a more international research language than the style I am used to.

All in all I can say that I enjoyed writing this bachelor thesis and I especially enjoyed conducting the interviews. To those who were so kind to answer my questions, a big thank you is directed for providing research data.

I wish you a good read,
Kind regards,

Robert-Jan G. Ruifrok

Summary

Throughout history wars have been upon humans. Whether they were small disputes or large world wars, often some sort of relationship with water is present. Poisoning a well by throwing a corps into its depth or puncturing a flood defence and creating such circumstances that troops could barely proceed are only two examples.

However, since the last century a different 'enemy' has seriously stepped onto the stage of war. These so called terrorists have not only the potential to spread destruction, but more so fear. Terrorism is not about killing, it is about impact (personal communication E. Bakker, 2013). This impact directed at the second most important element after oxygen in life, being water, is worth investigating. In the Netherlands it is especially of interest as the country lies under sea level while it is often seen as a legitimate target for international orientated jahidistic groups and networks (personal communication "Mijke"(AIVD), 2013). This because of the Dutch political and military presence in Afghanistan and other Islamic countries. On jihadistic webforums the Netherlands is depicted as discriminating against moslims.

But to what extent is the terrorist threat directed at watersystems in the Netherlands realistic, is it identified by the authorities and which measures are taken against these threats?

By creating a conceptual model as seen in chapter 2.3 assumptions are derived from the researched theory written on the subject. During the preperation of this theoretical framework it became clear that not a lot was written on the subject, which made the research exploratory orientated.

To test the conceptual model (in other words, the different surrounding factors that have a positive or a negative influence on the real chance of an effective terrorist attack on a Dutch water system) a qualitative method was used. By interviewing key positions around the subject the main question is answered. These key positions create a triangular view. One view coming from the water sector (among others both Rijkswaterstaat and drinking water sectors were interviewd), one view coming from academics who are experts in terrorism (a professor in (counter-) terrorism and a professor in conflict analyses) and a final view from policy makers (the General Intelligence & Security Service (AIVD) and the National Coordinator for Security & Counterterrorism (NCTV)). This way the interview questions filtered from the conceptual model could be submitted to different opinion holders and provide a good base for discussion.

By using the interview guide (see attachment I) and analysing the interview transcripts results gradually presented itself. By using a coding book (see attachment II) and selecting different pieces of transcript, answers to questions could be categorised and explained.

Regarding the realistic chance of a terrorist attack aimed at the water system of the Netherlands, the results from the research show that the odds are small. The policy makers, the actual water sector and the different experts agree on this. The policy makers state that

the *sector drinking water* and the *sector tunnels & flood defences* are at this moment at the 'standard' threat level which is the lowest in the set of four of the Dutch Counterterrorism Alert System (ATb). But by mentioning these two critical infrastructures, they at the same time agree to the existence of some sort of possible threat directed at these sectors.

The conclusions for both water sectors are different. The *sector tunnels & flood defences* is not very afraid of an actual threat or attack and have a sober and pragmatic approach to the matter, even though the accessibility to the Dutch water systems is relatively high and damage via destruction or bio- or chemical means is relatively simple. They believe that if a threat or attack would occur, the actual damage would be containable. The possible threat could consist of an actual attack using a bomb to destroy a part of the water system or reducing the quality of water in such a way that it would not be fit to be used as a primary source of drinking water, or no longer be safe for flora and fauna. For the *sector tunnels & flood defences* an agent that lowers the quality of surface water is easily washed away to the sea. While any physical damage could quickly be repaired with no or only few casualties.

The *sector drinking water* however is a different matter. Rijkswaterstaat reports that the water companies that use surface water, only need to close their inlet valves for a short period to keep the low quality water out. However, from the data that was collected, or rather not collected at the water companies, the conclusion can be drawn that this is possibly the most scared group of interviewees. There is however no need for this fear. First of all, the drinking water system in the Netherlands has many sources, thus sufficient physical accessibility to have an effective impact is difficult to achieve. When a facility would be hacked, polluted or destroyed another company could easily take over. Secondly, the system is complex and has many checks and controls that would be difficult to influence sufficiently for a total breakdown of even one water company.

The policy and security system for counterterrorism that is now in place in the Netherlands is vast. There are 15 sectors that have been mapped as critical infrastructures and two of these are water related. Thus specific infrastructural water protection and policy by the government, which is one of the important items in the conceptual model, is high which decreases the real chance of an effective terrorist attack on a water system to a great extent. Communication lines are set up and important actors are connected to each other via the NCTV.

The best chance on a successful attack is when an insider would exist with bad intentions or a person with bad intentions with access to critical control rooms, either digitally or analogue. However, since the 1st of January 2012 the National Cyber Security Centre (NCSC) is limiting the digital access of all Dutch governmental institutes to keep curious unwanted parties out. Therefore, as the different experts report, an insider is needed to create a threat or an actual attack on the Dutch water system. Sabotage by a frustrated employee is a bigger threat than a terrorist attack.

All in all, it is unlikely that a terrorist organisation would, to achieve maximum impact with its limited resources, choose a Dutch water system. And even if they would decide to do so, the effects would be small.

Table of contents

1. Introduction

1.1 Motive

Wars and threats dominate history books and tell us stories about disputes between city-states concerning land, food or even women. When we read this history, city-states that after a while evolve into countries, fight each other about economy, religion or loyalty. During all these wars, different methods have been used to overthrow the enemy. In the popular stories water often plays a dominant role (e.g. the West Indy Trading Company or the Second World War). This is not so odd as it seems, for water is the second element that is essential for life after oxygen. Therefore, using water as a mode of transport (as done during the Golden Era) or creating a short term abundancy, scarcity or even poisoning water was a proven military technique. As an example there is the old Dutch defence system, known as the Dutch Water Line, built in 1569. In 1573, at the beginning of the Eighty Year War against Spain, the Dutch flood the land to protect Leiden. This same type of national protection was used again by the Dutch but also by the Belgiums during the Second World War (Dutch Water Line, 2002). One might think that military disputes using water as a weapon are from a by gone era, however, using water as an offensive weapon has been used even throughout the 21st century. In 2009 North Korea released 40 million cubic meters of water from the Hwanggag dam, which caused a flash flood on the Imjin River which flows into South Korea. In South Korea, at least six fishermen and campers drowned. South Korea still fears that North Korea could use the water from the dam as a weapon during a violent conflict, though North Korea claimed that the water had to be urgently released and promised to warn the South of future releases in advance (Chloe, 2009).

Since the Second World War, not only countries have been fighting amongst each other, but other non-governmental players became important too. These players, such as the German RAF, developed warfare techniques we nowadays call terrorism. Terrorism has slowly become a more important player in our daily lives. Water is potentially an interesting element to perform terrorism with as clean drinkable water is scarce and can be easily manipulated. Also cyber terrorism is on the rise which could damage critical infrastructural aspects used by any society. Finally, the old fashioned way of destroying dams, tunnels or flood defences is still more or less present (personal communication E. Bakker, 2013).

The threat of terrorism is something a lot of the people in the world live with on a daily basis. When taking out a new insurance nowadays there is a part of the policy that talks about terrorism. When visiting a international airport or trainstation the terminalspeakers ask you not to leave personal belongings behind. When looking at the movies of last year and even this year created by large production companies from Hollywood there are some concerning terrorism. 'Zero Dark Thirty' is a film based on true events about the finding and

capture of former al-Qaeda leader Osama bin Laden. 'Olympus has Fallen' is a fictional story of an infiltration and a direct attack on the White House in Washington organised by a North Korean militant group. These production companies have a large amount of money reserved for advertising and getting the teasers, trailers and posters to as many people in the world as possible. Even in best seller books such as the last of author Dan Brown called 'Inferno', water terrorism was implemented in the story and even named. When looking at these subjects from a shallow viewpoint, not a lot would seem troublesome. However, with these actions and policies, one might say that whether the threat of terrorism is real or not, it is somehow present.

Nowadays, when a threat or even war is upon a country, the first targets one could think of when being attacked are military compounds (personal communication J. Dalebout). Nevertheless, there are many different (public) services that depend on freshwater and water infrastucture that when harmed, could damage the commercial and industrial economy. These water systems are potential targets for terrorism and the chance that terrorist will strike at water systems is real (Gleick, 2006). There are different possibilities to target a water system. Firstly, direct targeting. Dikes, waterlocks, ports, fresh water supply plants, sewage treatment plants and pumping stations are all possible targets for destruction or take-over (via the computer systems that control them). The possibility of a breach in waterdefences of for instance the Netherlands (where the majority of its land mass lies below sea level) has been investigated (Nederland van Boven, VPRO). Potentially this could harm many people.

Secondly, contamination through the introduction of poison or disease causing agents. Terrorists could poison the watersystem at fresh water supply plants, or closer to the user of the resource somewhere in the complicated supply lines. The difference with a direct military target such as an airport is that a water system attack makes water unusable or creates a shortage of water. More uncertain, however, is how significant these threats are nowadays compared with other targets that may be subject to terrorist attack. Or how effective these attacks would actually be. Analyses show that the chance of a large scale effect (either by direct destruction/take-over or by some form of poisoning) is not easy to achieve, although history has shown us a few exceptions (Gleick, 2006). Even so, the social impact of even a small event, especially when known to the general public, may cause a lot more disarray than thought.

This research intends to provide a good look at the different theories on water and terrorism and water system vulnerabilities. It will look at where potential risks could be present at the Dutch water systems as water is one of the most important resources for any country, and whether the risks are known, realistic and vital. If there is some degree of risk, current policies and defences will be checked.

1.2 Research objective

This research project will be exploratory-oriented. Not much literature is available regarding the relation between water and terrorism. Much can be found on bio-terrorism and eco-terrorism such as D.A. Handerson has done in 1998 in an article called "Bioterrorism as a public health threat". The currently proposed research, however, is meant to provide knowledge and information that can contribute to the theory of water terrorism by looking at whether there are potential terrorist threats that concern water, and to see how the Netherlands have armed themselves against these potential threats.

The objective of this research project is mapping potential terrorist threats aimed at water systems in the Netherlands in order to analyse how realistic such a potential threat actually is, afterwhich it will be investigated whether this is identified by the authorities and appropriate measures are taken.

Primary question
From the research objective, the research questions are filtered. First the primary question is formulated that should create the socalled 'red line' within the research. This central question will then be elaborated further using secondary questions. The central question is as follows:

To what extent is the terrorist threat directed at watersystems in the Netherlands realistic, is it identified by the authorities and which measures are taken against these threats?

Secondary questions
The central question is split into three secondary questions:

(i)   **To what extent are Dutch water systems vulnerable to terrorist attacks?**

(ii)   **In theory, to which extent can a terrorist attack targeting water systems take place and be succesfull?**

(iii)   **If the threat is real, is it recognised and what measures are taken into account?**

Research framework
A research framework is a schematic representation of the research objective and includes the appropriate steps that need to be taken in order to achieve it. Once such a scheme has been drawn up, the structure of the research plan is clear. It shows clearly how the different phases of the research are interconnected, and how the one step implies the other. In short, the research framework represents the internal logic of a research project (Verschuren & Doorewaard, 2010, p. 65).
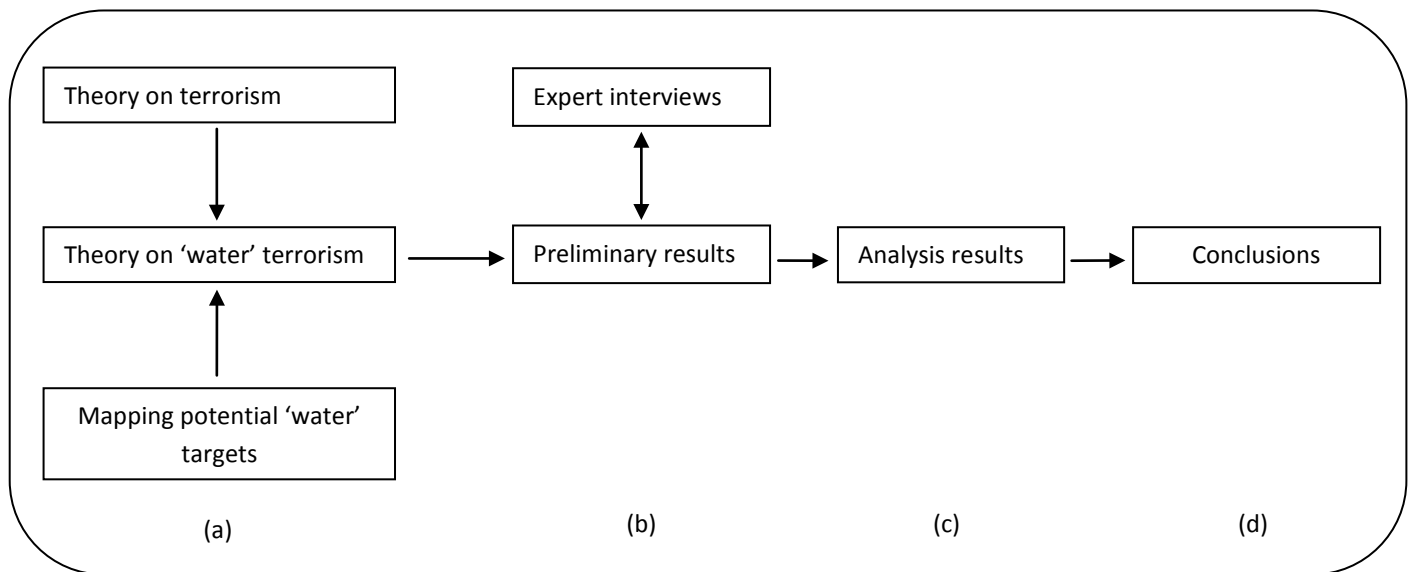
Figure 1. Research framework scheme
(a) A study of the available theories on terrorism, water security and biological and chemical terrorism directed at water systems, and mapping of potential targets. (b) Where different experts interviews from different viewpoints will contribute to the preliminary formulated results. (c) All the results are analysed and ordered. (d) Conclusions will be drawn to create a better insight concerning water terrorism in the Netherlands.

1.3 Scientific and social relevance

The research that will be conducted has a scientific relevance, as the objective is to create more theory on the subject of environmental and water terrorism since there has not been written a lot about this subject. The research will, because of the lack of information, be exploratory orientated. Terrorism destroys our sense of safety and normality and introduces new and often substantial stress and uncertainty in individuals and communities (Ursano *et al*., 2003). The social importance of this research is therefore present when investigating the role of terrorism and water.

When talking about terrorism in the Netherlands, there are all sorts of programmes and policies that are aimed specifically at terrorism and counter terrorism. Fifteen sectors have been marked by the authorities as being critical infrastructural areas. For each specific sector scripts have been developed (Personal communication J. Dalebout, 2013). This shows that the Dutch people and the Dutch government have the issue clearly on the agenda. The possibility of an attack on a water system of whatever kind is considered realistic (Personal communication E. Bakker, 2013). Since the increase of the Dutch national threat level from 'limited' to 'substantial', a larger interest in the matter has been taken. Investigating water and terrorism in the Netherlands is in particular of interest since a major part of the Netherlands lies under sea level which adds to the scientific and societal relevance.

2. Theoretical framework

2.1 The threat of terrorism

What is terrorism?

As many previous observers have noted, defining "terrorism" is problematic (Gleick, 2006; Wardlaw, 1989; Martin, 2006). A detailed review of the challenges of defining "terrorism", especially in the context of water systems, is provided by Gleick (2006: Chapter 1). No standard or consistent definition is used by federal or state agencies in the United States, although most follow the form of that adopted by the US Federal Bureau of Investigation (FBI): "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (US Code of Federal Regulations (28 CFR Section 0.85)). Similarly, the National Coordinator for Security and Counterterrorism (NCTV) in the Netherlands uses the following definition: "Terrorism is defined as threatening, making preparations for or perpetrating, for ideological reasons, acts of serious violence directed at people or other acts intended to cause property damage that could spark social disruption, for the purpose of bringing about social change, creating a climate of fear among the general public, or influencing political decision-making." Both of these definitions focus on motive – the "furtherance of political or social objectives". Such motives can also include religious, cultural, economic or psychological factors. Increasingly important, however, is the question of targets. In traditional discussions about terrorism, targets are usually governments, political figures, objects of economic or social significance, or random civilians. But both motives and targets can include environmental and ecological resources such as water and built water systems. The social and cultural value and importance of water systems also make them attractive targets. By calling attention to the inability of governments to protect vital symbols of civilization, terrorists can raise doubts about controlling authorities. As Thornton (1964) noted: "The relatively high efficiency of terrorism derives from its symbolic nature. If the terrorist comprehends that he is seeking a demonstration effect, he will attack targets with a maximum symbolic value." There are few natural resources with more symbolic power than water (Gleick, 2006).

The threat

The typical scenario for a terrorist attack on domestic water supplies involves putting a chemical or biological agent into local water supplies or using conventional explosives to damage basic infrastructure such as pipelines, dams and treatment plants. This is not as straightforward as it sounds (Gleick, 2006). The number of casualties that would result from such an attack depends on the system for water treatment already in place, the type and dosage of poison ingested, individual resistance, the timing of an attack and the speed and scope of discovery and response by local authorities.

Most biological pathogens cannot survive in water (Gleick, 2012) and most chemicals require very large volumes to contaminate a water system to any significant degree. Many pathogens and chemicals are vulnerable to the kinds of water treatment used to make it potable for human use. Indeed, the whole purpose of municipal water systems is to destroy biological pathogens and reduce the concentration of harmful chemicals through chlorination, filtration, ultraviolet radiation, ozonation and many other common treatment approaches. Many contaminants are also broken down over time by sunlight and other natural processes. Most infrastructures have built-in redundancy that reduces vulnerability to physical attacks. Because of these safeguards, one early commentator noted: "it is a myth that one can accomplish [mass destruction] by tossing a small quantity of a 'super-toxin' into the water supply. It would be virtually impossible to poison a large water supply: hydrolysis, chlorination and the required quantity of the toxin are the inhibiting factors" (Kupperman & Trent, 1979). It is important to note, however, that terrorist attacks that fail to kill or injure large numbers of people may still have important political repercussions by affecting public perception, reducing confidence in institutions and forcing inappropriate political responses. Society reacts differently to natural and human-caused disasters: we often accept large casualties from natural disasters with a degree of sanguinity not matched by our response to intentional acts of violence (Wardlaw, 1989). Terrorism destroys our sense of safety and normality and introduces new and often substantial stress and uncertainty in individuals and communities (Ursano *et al.*, 2003). Even a plausible public threat has the potential to cause fear and anxiety. The best defences against such threats are public confidence in water management systems, rapid and effective water quality monitoring, and strong and effective information dissemination (Gleick, 2006).

Infrastructure attacks and chemical and biological attacks

The most traditional form of water-related terrorism involves physical attacks on water infrastructure – specifically water-supply dams and pipelines. One such attack might target a large hydroelectric dam on a major river or a major water supply system for a city. Even a large dike ring could be targeted. Terrorists equipped with a relatively small conventional explosive might not be able to cause serious structural damage to a massive dam, which is, after all, usually a giant block of rock, earth or concrete. But the adverse consequences of a major dam failure make the risk worth both assessing and reducing. A major dam or dike failure can kill thousands of people and even more modest damage might interrupt power generation or affect some other important water system operation (Gleick, 2006). A more modern infrastructure concern is the use of remote computers to attack valves, pumps and chemical processing equipment though computer-based controls. If a group or individual could gain control over the automated operations of water facilities, water supplies or quality could be seriously compromised. These control systems were typically developed with no attention to security. As a result, many of the supervisory control and data acquisition (SCADA) networks used by water agencies to collect data from sensors and control equipment "may be susceptible to attacks and misuse" (Heilprin, 2005).

Of growing concern is the risk of chemical and biological attacks on water systems. This type of attack is often portrayed as follows. Terrorists introduce water-soluble biological or chemical contaminants into a publicly accessible city water supply. In the best-case scenario, the contaminant is detected as it enters the fresh water supply plant and the plant is shut down while the contaminant is neutralized. This can result in interruption of potable water service to the city and a "boil water" alert for city residents. In the worst-case scenario, the contaminant is undetected and people begin to get sick, panic ensues and health and economic damages soar. Chemical and biological attacks on water may not be as easy as often portrayed. In order to be effective as a tool of water-related terrorism, a chemical or biological weapon must be:

- **Weaponised**: it must be produced and disseminated in quantities sufficient to have the intended effect.
- **Appropriate for water dissemination**: it must be viable, dissolvable, stable and transportable in water.
- **Infectious, virulent or toxic**: it must be effective at causing illness or death, with no widespread immunity in the target population.
- **Effective over time and treatment**: it must maintain its effectiveness in water long enough to reach and affect humans and it must not be negated by standard water treatment systems likely to be in place (Gleick, 2006).

2.2   Eco- and water terrorism

Important distinctions should be made between two different categories: environmental terrorism and eco-terrorism. In recent years, US law enforcement agencies have had to deal with a range of concerns and activities increasingly defined as "terrorism" with an environmental or ecological context. For example, in 2006 the FBI announced arrests in several cases of property destruction thought to have been caused by extreme animal rights groups with "environmental" agendas. Indeed, FBI Director Mueller said one of the Bureau's "highest domestic terrorism priorities" is prosecuting people who commit crimes "in the name of animal rights or the environment" (Janofsky, 2006). This kind of activity, however, should be considered "eco-terrorism", not "environmental terrorism" (Schwartz, 1998; Schofield, 1999). There is an important distinction between the two. The term "environmental terrorism" should exclusively refer to the unlawful use of force against environmental resources or systems with the intent to harm individuals or deprive populations of environmental benefit(s) in the name of a political or social objective. This distinguishes it from "eco-terrorism", which should only be considered the unlawful use of force against people or property with the intent of saving the environment from further human encroachment and destruction. The professed aim of eco-terrorists is to slow or halt exploitation of natural resources and to bring public attention to environmental issues (see

Lee, 1995; Chalecki, 2001). Simply put, environmental terrorism (of which water terrorism is an example) involves targeting natural resources for a political, social or economic objective. Eco-terrorism involves targeting social, political or economic resources for an environmental objective. The former is the subject of this research (Gleick, 2006).

2.3 Conceptual model

On this page a conceptual model of the surrounding factors of complex interdependencies mentioned by theory is presented. A well-designed conceptual model should serve two purposes. It helps the researcher to demarcate clearly his or her research subject, and most importantly, the conceptual model supports the researcher to formulate the assumed relationships between the core concepts correctly, and to link the research project to an existing theory. The table below has been created with a clear research direction based on the theory found in chapter 2.1 and 2.2. All boxes marked with a C need to be investigated to see whether the literature that has been written and discussed in chapter 2.1 and 2.2 is of relevance to the Netherlands. This is done by interviewing key actors which will be explained in more detail in chapter 3, methodology and shown in the interview guides in attachment I.
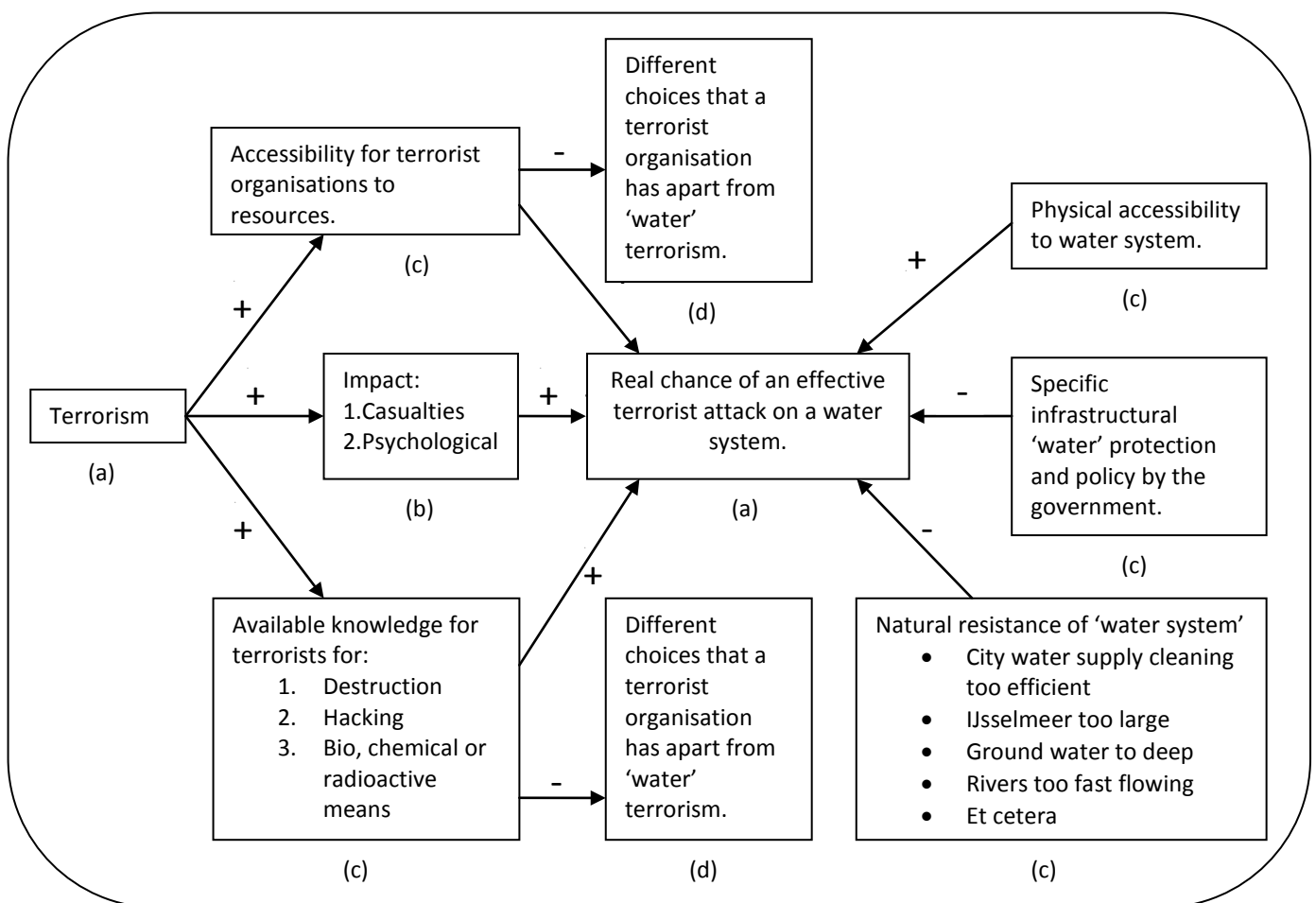
Figure 2. Conceptual model scheme
(a) All parts marked play a key role within the research, and form the research results. (b) Shows the specific goal the terrorist group has. (c) All circumstances that might negatively or positively add to the effectiveness of a terrorist attack extracted from chapter 2. (d) When a terrorist group would move away from the idea of water terrorism.

Definitions of central concepts

Concept	General definition	Stipulate definition
Water conflict	A situation where political or military confrontations occur in relation to water, either caused by discord about the quality, quantity or the distribution of water (Gleick, 2012; Harmsen 2006).	In this research, a water conflict will be defined as a situation where water is actually used as a target directed at state actors coming non-state actors.
Terrorism	Terrorism is defined as threatening, making preparations for or perpetrating, for ideological reasons, acts of serious violence directed at people or other acts intended to cause property damage that could spark social disruption, for the purpose of bringing about social change, creating a climate of fear among the general public, or influencing political decision-making (Martin, 2006; NCTV, 2013).	In this research, terrorist organizations are seen as both national and international non-governmental players that have a specific goal using violence to obtain it.
Biological and chemical weapons (including radioactivity)	Biological weapons are biological toxins or infectious agents such as bacteria, viruses, and fungi with intent to kill or incapacitate humans, animals or plants as an act of war. A chemical weapon is a device that uses chemicals formulated with intent to kill or incapacitate humans, animals or plants as an act of war (Gleick, 2012; Ursano 2003).	In this research, biological and chemical weapons are weapons that could be implemented by terrorist organisations at an international level.
Environmental terrorism	This should exclusively refer to the unlawful use of force against environmental resources or systems with the intent to harm individuals or deprive populations of environmental benefit(s) in the name of a political or social objective (Gleick, 2012; Janofsky, 2006; Schofield, 1999; Schwartz, 1998).	In this research, the general definition is used.
Water systems	From surface water (river or lake) to actual treatment plants with the entire infrastructure around it (Gleick, 2012; Lee, 1995).	In this research the entire infrastructure concerning fresh and saltwater is meant. From sewage treatment plants (STP's) to dams that hold off the sea.

3. Methodology

In the methodology chapter the research materials will be discussed together with the hermeneutic analysis of the expert interviews using the computer program ATLAS.ti.

3.1 Research strategy

This research project is an inventory of different theories already written, combined with conclusions created from different interviews conducted at key positions in the Dutch world of water and terrorism (see chapter 3.3). The research will have a contemplative and interpretive nature. The results of the different interviews are of qualitative nature and will therefore not contain calculations nor 'hard' numbers.

As will more thoroughly be explained in chapter 3.2, the different research methods are: literature research, using existing literature and secondary research.

3.2 Research materials and methods

In this paragraph it is stated for every research question what the research subject is, what kind of information needs to be collected, which sources will be used and how the information will be processed.

Main question: **To what extent is the terrorist threat directed at watersystems in the Netherlands realistic, is it identified by the authorities and which measures are taken against these threats?**

- Research objects: Improving the knowledge and theory regarding water terrorism in the Netherlands.
- What kind of information: texts, tables charts and images.
- Sources: literature and expert interviews.
- How to unlock: search systems, snowballing.
- How to process: filtration of data, hermeneutic analysis, summery transcriptions.

(i)   To what extent are Dutch water systems vulnerable to terrorist attacks?

- Research objects: inventory of Dutch water systems, their relative accessibility (physical and IT systems) and their natural resistance to the several types of terrorist attacks (destruction, hacking and bio- or chemical means).
- What kind of information: tables and charts.
- Sources: literature and experts interviews.

- How to unlock: search systems, snowballing.
- How to process: filtration of a large set of data into a small set of relevant combinations of targets/attack methods.

(ii)   In theory, to which extent can a terrorist attack targeting water systems take place and be succesfull?

- Research objects: attractiveness of targeting a water system versus other choices that a terrorist organisation has (resources, knowledge and impact, both in number of casualties as in psychological effects).
- What kind of information: qualitative information on means and methods of terrorist organisations.
- Sources: literature and expert interviews.
- How to unlock: search systems, snowballing and contacts.
- How to process: hermeneutic analysis (expert interviews), summary transcriptions (literature on terrorist theories).

(iii)   If the threat is real, is it recognised and what measures are taken into account?

- Research object: Overview whether the authorities recognise where the main terrorist attacks could happen, of what type they could be and whether they have made the right precautions against them.
- What kind of information: qualitative information on means and methods of authorities.
- Sources: literature and expert interviews.
- How to unlock: search systems, snowballing and contacts.
- How to process: hermeneutic analysis (expert interviews), summary transcriptions (literature on policies).

3.3 Observation methods

Several observation methods have been chosen to meet the research strategy. According to Verschuren & Doorewaard (2010) a combination between several methods is preferred. The following methods of data collection are used in the study: literature data and expert interviews. Below is an elaboration of the methods.

Literature data

Literature data collection is a form of desk research. Through literature review, the theoretical framework will be developed. Key concepts in the conceptual model are developed through this theoretical framework. Literature helps to achieve new insights (Verschuren & Doorewaard, 2010, p. 201). An important feature of the literature is that one uses the materials produced by others. Under literature we understand books, articles, journals, scientific papers and other forms where scientists share their knowledge. The biggest advantage of literature is that within a short period of time a large amount of data can be collected. Terms that will be sought to include are: non-state actors, terrorism, threats, water policy, water systems, security and military targets / tactics. A disadvantage of working with literature is that the information available on relatively new topics is still limited. For this reason, this method has been chosen to be combined with expert interviews.

Expert Interviews

An expert interview is a variant of the elite interview. This involves interviewing people who are knowledgeable about certain issues (Baarda, De Goede en Van der Meer-Middelburg, 2007, p. 19). The expert interviews are used to generate new information and may also serve to support knowledge that is extracted from the literature. Expert interviews may be conducted at the National Coordinator for Security and Counterterrorism (NCTV), the General Intelligence and Security Service (AIVD), terrorism experts and water safety experts. These (semi-) governmental institutions should provide a basis of knowledge as they are all somehow connected to the main or secondary questions. When looking at the key words (terrorism, water and target) the above interviewees can definitely provide some sort of information or knowledge. An example of a question that could be asked is: 'Is there a real threat that terrorist would attack water systems in the Netherlands?'. For a full list of questions see attachment I (interview guides).

When analysing research data some important steps need to be taken first (Creswell, 2007, p. 180). These steps are successively preparing and organizing the data. This applies to the interviews from which transcripts are created. The next step is to reduce the data into themes. This is done by encoding. The final step is to represent the data. This can be in figures, tables, or in the form of a discussion (Creswell, 2007, p. 180).

Besides the general steps that have to be applied during analysis, a number of more specific steps need to be taken into account. First, a description and the context of the particular interview must be presented. After that Creswell (2007, p. 199) distinguishes two types of data analysis. These are "categorical aggregation" and "direct interpretation". The difference between these types of data analysis is that "categorical aggregation" searches through the transcripts for various specific interview data which occur several times, after which something meaningful should present itself. An example would be critical infrastructures mentioned by the interviewed parties.

In "direct interpretation" a particular form of interview data which occurs only once, can influence the entire research because a certain interpretation is connected to the data (Creswell, 2007, p. 199). For the analysis of this research "categorical aggregation" is chosen. This was decided because we will be searching for similarities between the various interview data. The next step is to look for patterns. The goal is to find relationships between the categories created earlier. Finally, a 'naturalistic generalization' will be applied to these findings to make them of general value (Creswell, 2007, p. 200).

Who to interview?

To collect information on each secondary question as shown in chapter 3.2 of this research, objectivity would need to be acquired. To do so the data acquired in one particular field is checked with another data source from the same field to create a one directional view. This view can then be questioned by another opinion from another field, also derived from two independent sources. In this research a triangular view is created on all questions asked. One view comes from the water sector from interviewees who have a specific interest in the subject of terrorism from a water perspective. This is called the water sector view. Another view comes from academics who are experts in terrorism and know the field of water in general. This is called the expert view. The last view comes from the policy makers who have an overall view on both terrorism and water. This is called the policy view.

Policy view

Expert view ←——————————————→ Water sector view
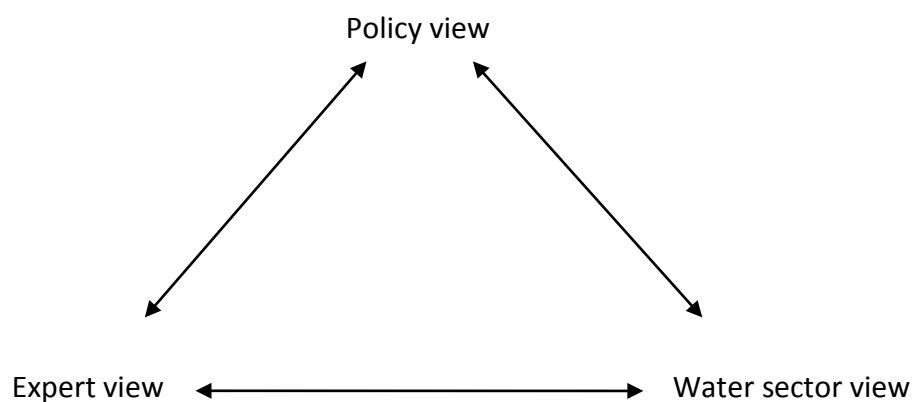
Water sector view

The water sector view comes from the water sector itself. This way data can be acquired by people that are actually in the field. This field is split up in two: *drinking water* and *tunnels & flood defences*.

1. Sabine Gielens. Secretary of the Security Committee & Crisis Management at the Association of Dutch Water Companies (in Dutch: Vereniging van Waterbedrijven in Nederland, VEWIN) (*sector drinking water*).

2. Lydia Barm. Adviser strategy at the water Company Evides in Rotterdam (*sector drinking water*).

3. Marrianne Krug. Policy adviser for e-government at the Association of Regional Water Authorities (in Dutch: Unie van Waterschappen) (*sector tunnels & flood defences*).

4. Jaap van Steenwijk. Coordinator crisis management at Rijkswaterstaat Transport- and Watermanagement in Lelystad (*sector tunnels & flood defences*).

Expert view

An expert view of the research and its questions are derived from interviews from two academics. By interviewing them an overall opinion is given, but is often more directed at the subject of terrorism.

1. Edwin Bakker. Professor (Counter-) Terrorism at the University of Leiden and director of the Centre for Terrorism and Counterterrorism in Den Haag.

2. Leon Wecke. Senior lecturer for the Centre for International Conflict- Analysis & Management at the Radboud University Nijmegen.

Policy view

The last overall view is provided by the policy makers that have been involved in the creation of policy around the subject of terrorism in the Netherlands.

1. J. Dalebout. Program manager Counterterrorism Alert System at the National Coordinator for Security and Counterterrorism (in Dutch: Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV) at the Ministry of Security and Justice.

2. "Mijke". General Intelligence and Security Service (in Dutch: Algemene Inlichtingen- en Veiligheidsdients, AIVD) at the Ministry of the Interior and Kingdom Relations.

For interview guides, see attachment I.

Software

For organizing and coding the data the computer program Atlas.ti was used. This program has the ability to create 'hermeneutic units' in which different types of data can be combined. Examples include transcripts of interviews, videos and images. Altas.ti offers the ability to select the data through open coding and can then bundle the selected data (or

codes) into themes called 'family codes'. This makes Atlas.ti a good tool in the analysis of the qualitative research data obtained (Creswell, 2007, p. 203).

When creating hermeneutic units in Atlas.ti, the following steps-by-step guide must be followed:

1.   What is the research question? What is our research interest? What is our theoretical background? What are our assumptions? What determines our choice of texts?

2.   What kind of protocol did the interview follow? From what form of interaction with the interviewee stems our text? What does it report? What relevant insight does one expect from it?

3.   Start the interpretation at the beginning of the text, where the scene is set for the rest (otherwise look for most relevant or contrasting parts).

4.   Take a short sequence and try to think of stories (sentences) in which the sequence fits well, until you cannot think of any substantially new 'story'.

5.   Try to categorise these stories according to their similarity and structure. This shows the optional structure of the speech act so far.

6.   Confront these options with the next sequence and see what 'choices' the speaker makes, and which options can be rejected.

7.   After this detailed analysis one can analyse other pieces of text in a faster way, in which the first interpretations serves as a kind of hypothesis.

8.   Meaning of interpretation for original theory.

The codes that have been used to analyse the interview transcripts can be found in attachment II, called the coding book.

4. Results

In this chapter the results are shown from the interview data. Important and relevant pieces of information are taken from the transcripts using the coding book (see attachment II). The data is then presented in this chapter using three separate paragraphs which are related to the three individual secondary research questions. At the end of each paragraph a preliminary conclusion is made.

4.1 Accessibility and natural resistance of Dutch water systems

To find the answer to the first secondary research question, interviews (see attachment I) have been analysed and coded (see attachment II) as explained in chapter 3. The root of these questions lays in the conceptual model in chapter 2.3. In this paragraph the results of the two surrounding factors being physical accessibility and the natural resistance of water systems to terrorist attacks are shown.

Inventory of Dutch water systems and their relative accessibility
Regarding the Dutch water system and its relative accessibility, one must first look at all critical infrastructural aspects. The Dutch government has made a list of 15 critical infrastructural sectors and two of these are water related. One is the *sector drinking water* (in Dutch: Drinkwater) and the other is *tunnels & flood defences* (in Dutch: Tunnels & waterkeringen). Structures falling in the category *tunnels & flood defences* are usually in public areas, not actively defended and relatively easy to access physically (personal communication J. van Steenwijk, 2013). Operational *tunnels & flood defences* are often connected to a computer system which makes them vulnerable to cyber-attacks. Skilled persons could hack into these different computer-controlled water systems (personal communication Marrianne Krug, 2013; Edwin Bakker, 2013). However, once inside the control of a dam or tunnel, one has to understand the system. Logging in or evading the security protocols might be easy for some, but once inside the actual program you have to understand it before you can actually use it. Often these computer programs are very complex and need specific skills to control (personal communication J. van Steenwijk, 2013).

When wanting to attack a fresh water supply line (*sector drinking water)*, the physical accessibility is very difficult (Lydia Barm, 2013; Sabine Gielens, 2013). Even when poisoning the fresh water supply chain, the chance of actual poisoned water coming out of taps in households is very small. There are simply too many checks and balances. Chances are effectively zero (personal communication Edwin Bakker, 2013).

In the west of the Netherlands fresh water supply plants seem better secured. However, this is not the case. In the west drinking water is often taken from surface water, which requires large fenced-off plants. In the east many more small pumping stations are

used taking water from groundwater sources, the large number and their interchangeability giving the required protection (personal communication Lydia Barm, 2013).

Natural resistance to several types of terrorist attacks

1) Destruction

By e.g. blowing up flood defences one could possibly create a catastrophe: a 5 meter difference in water level could be created flowing into one of the many polders. Such breach cannot be easily closed with for instance basalt blocks, they would just wash away. There are various possible scenarios ready to be implemented by Rijkswaterstaat to take care of such situations. For example, confiscating two inland vessels, tying them together, filling them with basalt blocks and sailing them into the breach. Then the remaining smaller breaches could be filled with more basalt blocks which would largely close the gap. After the strength of the flood has been decreased, a temporary system could close the breach entirely. This way construction of a new dam could commence and the remaining amount of water seeping through the temporary system could be pumped away easily (personal communication J. van Steenwijk, 2013).

2) Hacking

Many of the different small flood defences are operated manually, but the larger and more important systems can also be operated digitally. Most of the systems that are operated this way, have two different types of automated systems. When for instance water rises just a few meters, flood defences can be operated manually through a computer system. When the water has risen to a certain point (which is of course different for each defence system), flood gates could close automatically. Both these systems are often handled from a distance, which makes it vulnerable to hacking. The security used for the ICT components called SCADA has already been on the market for some time. There has also been some mentioning of this system on different media platforms. This means that if someone would want to hack the system, it would technically be possible (personal communication J. van Steenwijk, 2013).

However, the National Cyber Security Centre (NCSC), which started its activities in 2012, has improved cyber protection considerably (personal communication Marianne Krug, 2013). The AIVD estimates that cyberterrorists, even when able to hack the system, would not be able to cause sufficient damage.

3) Bio, chemical or radioactive means

A chemical, biological or radioactive attack on water systems is also a possibility. The scenario usually portrayed, is an agent in the publically accessible city water supply. In the worst case ever, 12 tons of a mix of potent pesticides was accidentally leaked into the river Rhine. In a factory from SANDOZ near Basel in 1986 an explosion occurred which, together with the fire extinguishing water, caused the 12 tons to flow into the Rhine. The effect of this accident was marginalised as the different shore states were immediately informed. They closed their drinking water inlet valves. The poisoned water washed away into the North Sea

where most of it was broken down or diluted. The effect it had on the flora and fauna was however considerable. An entire ecosystem was wiped out. A year later however, most of the ecosystem was more or less back in its former glory. Fresh water together with seeds and small fish from tributaries gave back the life that the main river had before. All it needed were nutrients, sunlight and opportunity from the tributaries to add new life (personal communication J. van Steenwijk, 2013).

Concluding: to what extent are Dutch water systems vulnerable to terrorist attacks?

The water sector can be split into two main groups, the *sector drinking water* and the *sector tunnels & flood defences*. The conclusions for both sectors are different. The *sector tunnels & flood defences* is not very afraid of an actual threat or attack and has a sober and pragmatic approach to the matter, even though the accessibility to the Dutch water systems is relatively high and damage via destruction or bio- or chemical means relatively simple (see conceptual model chapter 2.3). It is believed that if a threat or attack would occur, the actual damage would be containable. The threat could consist of an actual attack using a bomb to destroy a part of the water system. When this would happen on a small scale the impact would be minimal. When happening on a large scale at for instance a dike, Rijkswaterstaat has shown scenarios of tying up two inland ships and sailing them into the breach thus making effects rather limited. The threat or attack can also consist of reducing the quality of water in such a way that it would not be fit to be used as a primary source of drinking water, or no longer be safe for flora and fauna. For the *sector tunnels & flood defences* an agent that lowers the quality of surface water is easily washed away to the sea after closing the inlet valves. It could mean that part of the ecosystem would need time to restore itself, but this period would not be longer than one year.

The *sector drinking water* is a somewhat different matter. Rijkswaterstaat reports that the water companies that use surface water, only need to close their inlet valves for a short period to keep the low quality water out. Even when the fresh water supply chain itself would be poisoned, the chance of actual poisoned water coming out of taps in households is very small. There are simply too many checks and balances. The drinking water system in the Netherlands has many sources, thus sufficient physical accessibility to have an effective impact is difficult to achieve (see conceptual model chapter 2.3). A lot of water in the west is taken from surface water and in the east from ground water. The surface water often comes from one inlet source, but the ground water from many different sources. When a facility would be hacked, polluted or destroyed another company could easily take over. There are 9 water companies that could cover the demand if one would be out of order.

The best chance on a successful attack is when an insider would exist with bad intentions or a person with bad intentions with access to critical control rooms, either digitally or analogue (hacking, see conceptual model chapter 2.3). However, since the 1st of

January 2012 the National Cyber Security Centre (NCSC) has limited the digital access of all Dutch governmental institutes to keep curious unwanted parties out.

The natural resistance of the Dutch water systems is large, and their relative accessibility is in the case of the *sector tunnels & flood defences* also large. In the case of the *sector drinking water* the accessibility is very small.

4.2 Attractiveness of targeting water systems versus other options for terrorist attacks

Even though the *sector drinking water* in the Netherlands could be a legitimate target for terrorist organisations, networks and individuals, the General Intelligence and Security Service (AIVD) based on their knowledge and expertise thinks that the combination of intention and potential to commit a complex attack against this sector in the Netherlands is scarce. Nevertheless, the threat is conceivable and should not be excluded completely. This because on the jihadist internet calls are found to digitally attack SCADA systems at the Dutch vital sectors. However, such calls on web forums are no indication that preparations for operations are in effect (personal communication "Mijke"(AIVD), 2013).

Terrorists have often an addiction to forceful or 'cool' attacks: the bomb, the weapon, the quick fire, a Kalashnikov. Catastrophic terrorism has been on the rise since 9/11. Using water the chances of creating a catastrophic event that could potentially kill many people is small, however the economic effect could be large. Chances are also small when looking at the number and type of incidents in the past and the *modus operandi*, the preferences and mentality of a terrorist (personal communication Edwin Bakker, 2013). In addition, opportunity plays an important role and is a factor when terrorist groups, networks and individuals choose their target. When a target is for instance too heavily guarded for their capacity to organise a successful attack, it is conceivable that a different target is chosen (personal communication "Mijke"(AIVD), 2013).

To achieve a lot of impact, an actual weapon in a crowded area would probably be easier and quicker. If however, the aim of the attack is not to kill anyone, but just to scare, then a dirty bomb, something that would contain radioactive material, would be quicker to see such a result. Terrorism is not about killing, it is about impact (personal communication Edwin Bakker, 2013).

Concluding: in theory, to which extent can a terrorist attack targeting water systems take place and be succesful?

Most replies appear to converge. The General Intelligence and Security Service (AIVD) summerised this best in her quick and brief answer: "…the AIVD estimates based on our knowledge and expertise that the combination of intention and potential to commit a complex attack agains this sector in the Netherlands is scarce. However, the threat is conceivable and can not be excluded". However, this statement should not be believed at face value. Rijkswaterstaat presented a somewhat different story. There is a fair amount of risk when floods are simulated. See figure 3, 4 and 5 below.
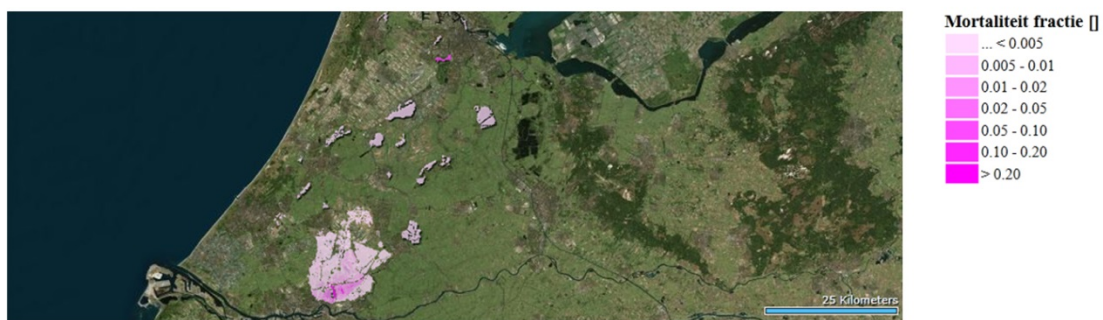

Figure 3. Mortality fraction
The above shows the output of a flood simulator developed by 'HKV Lijn in water' commissioned by 'Rijkswaterstaat'. This particular image shows the mortality fraction after a breach of dike ring 14 at the second flood defence of 'Boerengatsluis' near the city of Rotterdam. The deepest colour shows the area where more than 20% of the population will die due to a sudden simulated breach in the flood defences.
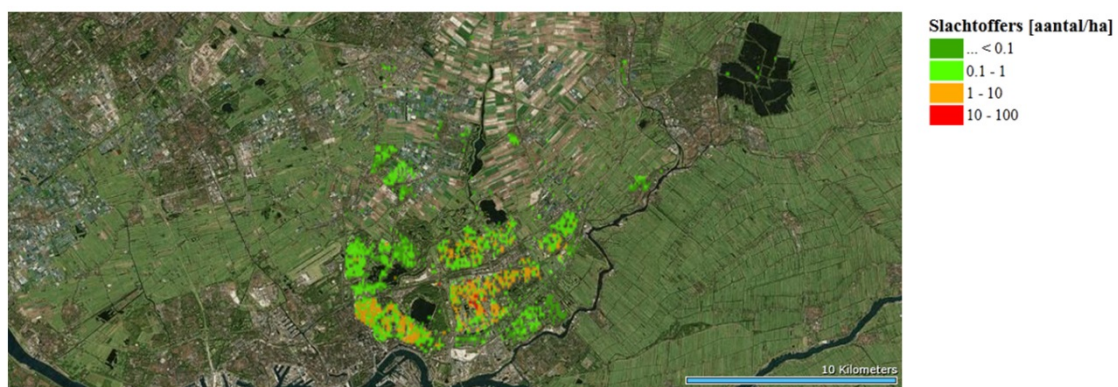
Figure 4. Victims (amount per hectare)
This particular image shows the amount of victims per hectare after a breach of dike ring 14 at the second flood defence of 'Boerengatsluis' near the city of Rotterdam. The colour red shows the area where between 10 and 100 people per hectare will be victimised due to a sudden simulated breach in the flood defences.
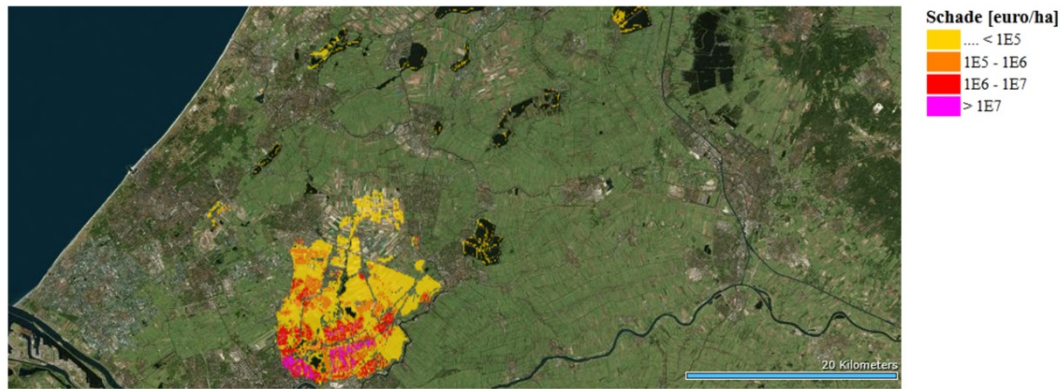
Figure 5. Damage (euro's per hectare)
This particular image shows the amount of damage in euro's per hectare after a breach of dike ring 14 at the second flood defence of 'Boerengatsluis' near the city of Rotterdam. The colour purple shows the area where more than 1 million euro's per hectare of damage will be done due to a sudden simulated breach in the flood defences.

These three images show that there is some degree of effect when a breach at the right time in the right place would occur. We can therefor conclude that nor the AIVD, nor the NCTV would want to spread information that the above is indeed possible. Of course, specific infrastructural 'water' protection and policy is implemented, which should prevent such an event to occur. This is explained in the next paragraph.

4.3 Overview of authorities recognition

First an overview is given explaining the general policies that exist concerning terrorism. After this overview the results are shown that cover the specific policies of the water sector.

General recognition

The chance of an attack in the Netherlands, or on Dutch interests on foreign ground has increased this year. The alert level as used by the NCTV is at this moment 'moderate'. The NCTV has heightened the alert level from 'limited' based on information from the AIVD (there are four possible threat levels: minimal, limited, substantial and critical). This is mainly because of signs of radicalisation among young people. Close to a hundred individuals have recently left the Netherlands for various countries in Africa and the Middle East, especially Syria. From Europe as a whole, many more have made the journey to join local armed groups (personal communication J. Dalebout, 2013).

The threat of international orientated jihadisst groups, networks and individuals has stayed unaltered. The Netherlands is still being percieved as an islamic hostile country and is therefor seen as a legitimate target. Also on the jihadistic internet the Netherlands is, with changing intensity, seen as a example of an islamic hostile western country.

The possibility of a terrorist attack in the Netherlands is 'moderate' because (personal communicatio "Mijke"(AIVD), 2013):

- In conflict zones like Syria, jihadist travellers acquire knowledge and combat experience and can pose a threat to Western interests. There is also a risk that they will inspire others in the Netherlands to follow in their footsteps. These jihadist travellers can return to the Netherlands highly radicalised, traumatised and with a strong desire to commit violence, thus posing a significant threat to this country.
- In addition, nascent democratisation in North Africa and the Middle East has resulted in greater freedom for these jihadist networks. The security organisations in these countries are no longer willing or able to offer resistance to these networks. It is easy for jihadist networks to establish themselves there. Some would like to attack Western targets, including in Europe.
- The Netherlands is (still) seen as a ligitimate target for international orientated jihadistic groups and networks because:
  - Dutch political and military presence in Afghansitan and other Islamic countries, and because of the support given to the Frensh intervention in Mali.
  - On jihadistic webforums the Netherlands are depicted as discriminating against moslims.
  - In November 2012 the Netherlands were called an example of an Islamic hostile country by a Somalic al Shabaab leader, Skeikh Fu'ad Shonhole.

o In the English jihadistic internet magazine "Inspire" of the 1st of March 2013, among others Geert Wilders and Ayaan Hirsi Ali are mentioned on the socalled 'hitlist'.

General precautions

Terrorist threat assessment Netherlands (DTN)

Terrorist threat assessment Netherlands (In Dutch: DTN) is a general assessment of the national and international terrorist threat to the Netherlands and Dutch interests abroad. The DTN is primarily intended for the administrative and political leadership and policymakers, using confidential information from the services responsible for fighting terrorism and radicalisation. Information from publicly accessible sources, administrative sources and the NCTV's own analyses is also used for this purpose.

The nature and seriousness of the terrorist threat is determined by many factors. In the Netherlands, four levels of ascending threat exist: minimal, limited, substantial and critical. The following table lists a number of factors that are used to determine the threat level. It is important to emphasise that the list is not exhaustive. It serves merely as an illustration.

Each threat level should in fact be regarded as a threat range without clear boundaries. This means that variations can occur in the nature, size and background of the threat without prompting a change in the general threat level. Factors may change, but the overall assessment remains roughly the same.

Level	Some relevant criteria
Minimal	National and international terrorist networks are barely present. It is unlikely that attacks are being planned. This threat level is sustained by the risks associated with maintaining an open and modern society.
Limited	There are now new trends or phenomena that constitute a threat. Activities by terrorist networks have been hindered. The Netherlands is seldom or never mentioned in statements issued by terrorist networks that pose a serious threat.
Substantial	New trends or phenomena that constitute a threat are discovered. There is a realistic possibility that an attack will occur in the Netherlands. Attacks are occurring in other countries that are comparable to the Netherlands. Radicalisation and recruitment are taking place on a significant scale. The Netherlands is frequently mentioned in statements issued by terrorist networks that pose a serious threat.
Critical	There are strong indications that an attack will occur in the Netherlands. An attack had taken place in the Netherlands and there is a strong possibility of follow-up attack. The Netherlands is frequently mentioned in statements issued by terrorist networks. These statements, which seriously threaten specific targets, should be taken very seriously.

(Source: NCTV 2013, http://english.nctv.nl/themes_en/Counterterrorism/)

Counterterrorism Alert System (ATb)

As mentioned before, the Dutch government has made a list of 15 critical infrastructural sectors and two of these are water related. After 9/11 a programme called Counterterrorism Alert System (in Dutch: Alerteringsysteem Terrorismebestrijding, ATb) was created. The ATb is an alert system for the government and economic sectors. It warns the operational services and economic sectors in the event of a heightened threat. The threat can consist out of possible economic damage, image loss or the loss of citizens. This enables prior measures to be taken quickly in order to minimise the risk of terrorist attacks in the Netherlands and to limit the potential impact of terrorist acts. The system is aimed solely at professionals who may have to deal with a terrorist threat. The National Coordinator for Security and Counterterrorism is responsible for the implementation, operation and overall management of the System. 15 economic sectors are currently connected to the ATb:

- Airports
- Railways
- Municipal and regional transport
- Seaports
- Tunnels & flood defences (currently at level 'standard')
- Chemical industry
- Oil industry
- Drinking water (currently at level 'standard')
- Natural gas
- Electricity
- Telecommunications
- Nuclear
- Finance
- Public events
- Hotels

The ATb has 4 levels of alerts: the standard level and 3 levels of ascending threat (low, moderate and high). Each level comes with its own set of security measures in each economic sector. As the level of alert rises, the security measures become more stringent and more far-reaching. The agencies concerned are free to vary their own measures according to the nature of the threat. They can take additional measures if necessary. The basic principle is to specifically tailor the measurements to meet the threat at hand. Together with the AIVD, the Ministry of Defence (MIVD) and the national information organisation for the national police (LIO) all sectors are updated annually (personal communication J. Dalebout, 2013). The four levels are determined by a different set of security protocols. The 'standard' level is organised by the sector itself. The 'low' level means that a sector should have a certain defensibility. For example, the sector uses security guards, places fences around the actual site, has a central keeper of the keys, has a 24 hour

surveillance *et cetera*. Of course these measures will differ per sector, as one could imagine that fences around a hotel would not be functional.

Crisis management

Standard crisis management has five phases, also in the case of terrorism. The NCTV uses:

1) Pro-action

    The NCTV organises the entire pro-action phase. The NCTV addresses different sectors and companies and ask them to sign an ATb connection document. This way they are obliged to organise different measures that the NCTV has come up with.

2) Prevention

    The prevention phase is actually an information phase. It only means that everybody is up-to-date using the latest intelligence gathered from different parties at the organisational meeting UOA. At this meeting per sector information is shared together with the AIVD, the MIVD and LIO. Safe and unhindered functioning of parts of the critical infrastructure is primarily the responsibility of the sector itself. However, it is also a responsibility of the government to prevent loss of public utilities such as the supply of drinking water. Therefore, the AIVD provides companies in the vital sectors information about (potential) threats and enables them to take measures to reduce their vulnerability, called targeted information (personal communication "Mijke"(AIVD), 2013).

3) Preparation

    The preparation phase starts when the first two phases are implemented. It is a phase where scenarios are actually practised for a possible event. It consists of training and education. Scenario writers create a possible story which is executed and analysed. During these exercises the different ATb levels can be adjusted to create a better system.

4) Repression

    The repression phase is the phase when there is a real threat based on actual information. Measures will then be taken based on an action plan which is alive and has been practised. The plan of action has been communicated with the different sectors beforehand in the prevention phase. These actions are fixed agreements and are in the form of a table. In case of a threat the table shows what the different teams should do (e.g. local government, police, *et cetera*).

5) Aftercare

    This is more or less the evaluation phase. The threat or event will be evaluated and the system will be checked. The different levels will also be evaluated and where needed adjustments will be made.

Sector drinking water

The current ATb level for the *sector drinking water* is 'standard'. This means that the threat level for the sector drinking water is at the moment lower than the DTN. The *sector drinking water* has been part of the ATb since 2005.

The AIVD created a group after 9/11 to create a package of 'standard' security measurements for the *sector drinking water*. Together with VEWIN, Vitens and Evides these measurements were implemented in the entire drinking water sector, and became later part of the ATb.

The sector and the police have per ATb level created a set of physical, organisational and personel measures that are executed according to the different types of threats. Alignment within the entire sector is achieved at organisational meetings (Uitvoeringsoverleg Alerteren, UOA) (personal communication J. Dalebout, 2013). Besides, the water supply companies are bound by law to guarantee supply, continuity, security, crisis management *et cetera*. Inspection regarding these guarantees is done by a service called: Environment and Transport Inspectorate (ILT) at the NCTV (personal communication L. Barm, 2013).

Sector Tunnels & flood defences

The current level for the *sector tunnels & flood defences* is 'standard'. The sector has been part of ATb since 2005. The sector and the police have per level created a set of physical, organisational and personel measures that can be executed according to the different types of threats. Alignment with the entire sector is done at the organisational meetings UOA at the NCTV.

Concluding: if the threat is real, is it recognised and what measures are taken into account?

The policy and security systems for counterterrorism that are now in place in the Netherlands are quite vast, detailed and efficient. As seen in the results there are 15 sectors that have been mapped as critical infrastructures and two of these are water related. Thus specific infrastructural water protection and policy by the government, which is one of the important items in the conceptual model, is high. This decreases the real chance of an effective terrorist attack on a water system to a great extent. The current threat level for the *sector drinking water* and the *sector tunnels & flood defences* is 'standard'. Every level has a specific table that shows what should be done by who in every situation. Different scenarios are practised, communication lines are set up and important actors are connected to each other via the NCTV.

5. Concluding remarks

5.1 Conclusions

From the Results chapter the following can be concluded with respect to the main research question which was:

To what extent is the terrorist threat directed at watersystems in the Netherlands realistic, is it identified by the authorities and which measures are taken against these threats?

Regarding the realistic chance of a terrorist attack aimed at the water systems of the Netherlands, the results from the research show that the odds are small. There is a distinct possibility of a threat being made or an actual attack executed. However, the chance of this occurring is very small as the policy makers, the actual water sector and the different experts agree on. The policy makers state that the *sector drinking water* and the *sector tunnels & flood defences* are at this moment at the 'standard' threat level which is the lowest in the set of four of the Dutch Counterterrorism Alert System. But by mentioning these two critical infrastructures, they at the same time agree to the existence of some sort of possible threat directed at these sectors.

The water sector can be split into two main groups, the *sector drinking water* and the *sector tunnels & flood defences*. The conclusions for both sectors are different. The *sector tunnels & flood defences* is not very afraid of an actual threat or attack and have a sober and pragmatic approach to the matter, even though the accessibility to the Dutch water systems is relatively high and damage via destruction or bio- or chemical means relatively simple (see conceptual model chapter 2.3). They believe that if a threat or attack would occur, the actual damage would be containable. The threat could consist of an actual attack using a bomb to destroy a part of the water system. When this would happen on a small scale the impact would be minimal. When happening on a large scale at for instance a dike, Rijkswaterstaat has shown scenarios of tying up two inland ships and sailing them into the breach thus making effects rather limited. The threat or attack can also consist of reducing the quality of water in such a way that it would not be fit to be used as a primary source of drinking water, or no longer be safe for flora and fauna. For the *sector tunnels & flood defences* an agent that lowers the quality of surface water is easily washed away to the sea after closing the inlet valves. It could mean that part of the ecosystem would need time to restore itself, but this period would not be longer than one year.

The *sector drinking water* however is an entirely different matter. Rijkswaterstaat reports that the water companies that use surface water, only need to close their inlet valves for a short period to keep the low quality water out. However, from the data that was collected, or rather not collected at the water companies, the conclusion can be drawn that this is possibly the most scared group of interviewees. This may be since both parties that

were interviewed for the *sector drinking water* spent a lot of time in the United States of America communicating with fellow colleagues about the issue of the act of terrorism that could occur at drinking water facilities. As the amount of theory that has been written on the subject mostly comes from America, Dutch drinking water companies may have copied this fear. Terrorist prevention in this sector in the USA is a multi-billion market involving more than 3000 companies and employing close to one million people in a market that has a turnover close to 50 billion dollars per year (Washington Post, 2010).

There is however no need for this fear. First of all, the drinking water system in the Netherlands has many sources, thus sufficient physical accessibility to have an effective impact is difficult to achieve (see conceptual model chapter 2.3). A lot of water in the west is taken from surface water and in the east from ground water. The surface water often comes from one inlet source, but the ground water from many different sources. When a facility would be hacked, polluted or destroyed another company could easily take over. There are 9 water companies that could cover the demand if one would be out of order. Secondly, the system is complex and has many checks and controls (including very extensive and efficient cleaning technologies) that would be difficult to influence sufficiently for a total breakdown of even one water company.

The policy and security system for counterterrorism that is now in place in the Netherlands is quite vast, detailed and efficient. As seen in the results there are 15 sectors that have been mapped as critical infrastructures and two of these are water related. Thus specific infrastructural water protection and policy by the government, which is one of the important items in the conceptual model, is high which decreases the real chance of an effective terrorist attack on a water system to a great extent. The current level for the *sector drinking water* is 'standard'. Every level has a certain table that shows what should be done by who in every situation. Different scenarios are practised, communication lines are set up and important actors are connected to each other via the NCTV.

The best chance of a successful attack is when an insider would exist with bad intentions or a person with bad intentions with access to critical control rooms, either digitally or analogue (hacking, see conceptual model chapter 2.3). However, since the 1st of January 2012 the National Cyber Security Centre (NCSC) is trying to limit the digital access of all Dutch governmental institutes to keep curious unwanted parties out. Therefore, as the different experts report, an insider is needed to create a threat or an actual attack on the Dutch water system. Sabotage by a frustrated employee is a bigger threat than a terrorist attack.

All in all, it is unlikely that a terrorist organisation would, to achieve maximum impact with its limited resources, choose a Dutch water system. And even if they would decide to do so, the effects would be small.

5.2 Recommendations for future policy and research

After examining the results and answering the main question, there is still room for future research. A large part of the Dutch critical infrastructure is linked to that of member states of the European Union. Therefore the possibility of a threat or an attack on either the *sector drinking water* or the *sector tunnels & flood defences* could also be investigated in other EU countries as this could have an effect on the Netherlands such as pollution of the river Rhine.

In this research only two critical infrastructures were investigated. To create a broader perspective, some of the other 15 sectors could be researched using the same principle design of research.

Last but not least research could be conducted as to whether the 'list of 15' made by the NCTV is up to date and does not miss a piece of critical infrastructure.

5.3 Critical self-reflection

When looking at the process that I have been through these last few months, I can only say that most of the time I have struggled with the more research orientated side of this study. From the start when creating the research plan the way academic research is executed was new for me. Therefore I learned a lot but I can also say that when I would conduct this research again, I would do parts differently.

To create a better picture of cyber terrorism an interview at the National Cyber Security Centre (NCSC) would need to be done. Extra information can be obtained about cyber security at critical infrastructural places in the Netherlands. The way this is handled from a digital perspective can add substantially to this research.

Also, to add to the data collected at drinking water companies, a real interview where all the questions are answered would considerably contribute to the research. The current data collected at drinking water companies is little. The problem is (as found) that drinking water companies do not give information away easily.

Lastly, a more flowing research would be better to show the reader how one chapter automatically leads to another. Often it helps to be clearer and more to the point, instead of describing with too many words the matter at hand. It is not intended for English literature.

References

Baarda, D.B., de Goede, M.P.M. & Teunissen, J. (2009). *Basisboek Kwalitatief onderzoek: Handleiding voor het opzetten en uitvoeren van kwalitatief onderzoek. Tweede druk.* Groningen: Noordhoff Uitgevers.

Baarda, D.B., De Goede, M.P.M. & van der Meer-Middelburg, A.G.E., (2007). *Basisboek interviewen: Handleiding voor het voorbereiden en afnemen van interviews. 2nd Edition*. Groningen: Noordhoff Uitgevers.

Chalecki, E. (2001). *A New Vigilance: Identifying and Reducing the Risks of Environmental Terrorism.* A Report of the Pacific Institute for Studies in Development, Environment, and Security, Oakland, California, online at
http://www.pacinst.org/reports/environment_and_terrorism/.

Cresswel, J.W. (2007). *Qualitative Inquiry & Research Design: Choosing Among Five Approaches. Derde editie*. London: SAGE Publications Ltd.

Flyvbjerg, B. (2006). *Five misunderstandings about case-study research*. Qualitative Inquiry, 2006, 219-245.

Gleick, P. H., Heberger, M., (2012). *The World's Water. The Biennial Report on Freshwater Resources. Volume 7.* Washington, Island Press.

Gleick, P. H. (2006). *Water and terrorism.* IWA Publishing, California.

Heilprin, J. (2005). EPA watchdog finds security lapses in remote controls for water systems. Associated Press, 10 January.
http://www.sfgate.com/cgi-
in/article.cgi?file=/news/archive/2005/01/10/national1827EST0682.DTL.

Janofsky, M. (2006). Feds accuse 11 of ecoterrorism: Targeted meatpacker, ski resort, timber firm. *New York Times News Service*, 21 January 2006.
http://homelandsecurity.osu.edu/focusareas/domestic.html.

Kupperman, R. H. & Trent, D. M. (1979). *Terrorism: Threat, Reality, Response.* Hoover Institution Press, Stanford, CA.

Lee, M. F. (1995). *Violence and the environment: the case of 'Earth first!' Terrorism and Political Violence*, 7(3), 109–127.

Martin, G. (2006). *Understanding Terrorism: Challenges, Perspectives, and Issues, 2nd Edition.* Sage Publications, Thousand Oaks, California.

National Coordinator for Security and Counterterrorism (2013). Summary of the National Terrorist Threat Assessment for the Netherlands (no. 32 of March 13, 2013).

National Coordinator for Security and Counterterrorism (2013). Counterterrorism Alert System. Finding date on 10th of April 2013: http://english.nctv.nl/themes_en/Counterterrorism/Counterterrorism_Alert_System/.

Priest, D., Arkin, W. M. (2010). *A hidden world, growing beyond control*. Washington Post 19th of July 2010. Finding date on the 13th August 2013, on: http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/1/.

Thornton, T. P. (1964). Terror as a weapon of political agitation. In *Internal War: Problems and Approaches.* Eckstein, H. (ed.). Free Press of Glencoe, New York, p. 73.

Ursano, R. J., Fullerton, C. S. & Norwood, A. E. (2003). *Terrorism and disasters: Prevention, intervention, and recovery. In Terrorism and Disaster: Individual and Community Mental Health Intervention.* Ursano, R. J., Fullerton, C. S. & Norwood, A. E. (eds). Cambridge University Press, Cambridge, United Kingdom, pp. 333–340.

Schofield, T. (1999). The environment as an ideological weapon: a proposal to criminalize environmental terrorism. *Boston College Environmental Law Review*, 26, 619–647.

Schwartz, D. (1998). Environmental terrorism: analyzing the concept. *Journal of Peace Research*, 35(4), 483–496.

Van Melik, R. (2012). *Visual Data Analysis.* Finding date on 22th feb 2013, on RU Blackboard: https://blackboard.ru.nl/webapps/portal/frameset.jsp?tab_tab_group_id=_3_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Flauncher%3Ftype%3DCourse%26id%3D_74912_1%26url%3D.

Verschuren, P.J.M. & Doorewaard, J.A.C.M. (2010). *Designing a research project. 2nd Edition*. Den Haag: Uitgeverij LEMMA.

Wardlaw, G. (1989). *Political terrorism, Theory, Tactics and Counter-measures, 2nd Edition.* Cambridge University Press, Cambridge.

Front page image found on the 12th Augustus 2013 on:

http://8tr.s3.amazonaws.com/i/000/454/933/wallpaper-background-atomic-water-bomb-graphics-code--h-t-ibackgroundz.com-2757.jpg found on the 12th of august 2013

Attachment I

Three examples of interview guides (In Dutch)

Interview gericht aan een terrorisme expert in Leiden op 25 april 2013
Tussen RJ.G.Ruifrok (student Radboud Universiteit)
En Edwin Bakker (Hoogleraar (Contra-)Terrorisme aan de Universiteit Leiden en directeur van het Centre for Terrorism & Counterterrorism in Den Haag)

1. Is de mogelijkheid van een terroristische aanslag überhaupt in Nederland reëel?
   a. Antwoord waarop gebaseerd?
   b. Antwoord kwantitatief laten zijn, niet alleen kwalitatief.
   c. Concreet, geen warrige verhalen accepteren. Doorvragen.

2. Is de mogelijkheid van een terroristische aanslag in Nederland, gericht op het water systeem reëel?
   a. Antwoord waarop gebaseerd?
   b. Kan men differentiëren tussen de verschillende water systemen, resp. de verschillende vormen van aanval?
      i. Bijvoorbeeld het vergiftigen (vergiftigen, klopt het wat Gleick zegt? Zou het niet kunnen dat er een super giftige stof in het waternetwerk wordt gegooid?)
      ii. Bijvoorbeeld het Hacken (het openen van sluizen of juist dichthouden)
      iii. Bijvoorbeeld het verwoesten (dijken, sluizen, watersystemen)
      iv. Zijn er niet veel installaties natuurlijk beschermd?
   c. Zouden ze niet sneller andere manier kiezen?
      i. Denk aan het conceptueel model
         1. Accessibility is misschien moeilijk bij watersystemen
         2. Terrorist heeft ook bepaalde kennis nodig, meer dan misschien bij andere mogelijke doelen.
   d. Antwoord kwantitatief laten zijn, niet alleen kwalitatief.
   e. Concreet, geen warrige verhalen accepteren. Doorvragen.

3. Wat kan er gedaan worden tegen zulke mogelijke aanvallen?
   a. Naar specifieke policy documenten/beleidslijnen vragen (kopieën beschikbaar?)
   b. Is er een indeling welke volgens jullie het meest mogelijk zijn?

Hoofdvraag
To what extent is the terrorist threat directed at watersystems in the Netherlands realistic, is it identified by the authorities and which measures are taken against these threats?

Deelvragen
(i)   To what extent are Dutch water systems vulnerable to terrorist attacks?
(ii)   In theory, to which extent can a terrorist attack targeting water systems take place and be succesfull?
(iii)   If the threat is real, is it recognised and what measures are taken into account?

Open interview gericht aan water sector tussen RJ.G.Ruifrok (student Radboud Universiteit)
En Sabiene Gielens (contact van de NCTV m.b.t. sector 'Drinkwater') (Vereniging van
waterbedrijven in Nederland)

1. Is de mogelijkheid van een terroristische aanslag in Nederland, gericht op het water
   systeem reëel?
      a. Antwoord waarop gebaseerd?
      b. Kan men differentiëren tussen de verschillende water systemen, resp. de
         verschillende vormen van aanval?
            i. Bijvoorbeeld het vergiftigen (vergiftigen, klopt het wat Gleick zegt?
               Zou het niet kunnen dat er een super giftige stof in de
               drinkwaterketen wordt gegooid?)
           ii. Bijvoorbeeld het Hacken (het openen van sluizen, inlaatkleppen etc. of
               juist dichthouden)
          iii. Bijvoorbeeld het verwoesten (dijken, sluizen, critische infrastructuur in
               het algemeen)
           iv. Zijn er niet veel installaties natuurlijk beschermd?
      c. Zouden ze niet sneller andere manier kiezen?
            i. Denk aan het conceptueel model
                  1. Accessibility is misschien moeilijk bij watersystemen
                  2. Terrorist heeft ook bepaalde kennis nodig, meer dan misschien
                     bij andere mogelijke doelen.

2. Wat vind u van het huidig beleid ten opzicht van terrorisme en/of policy makers zoals
   de AIVD, NCTV, Rijkswaterstaat? Bent u aangesloten bij het ATB.

3. Sinds wanneer is er een omslag het het veiligheidsbeleid van de verschillende
   drinkwaterbedrijven cq vewin.

4. Wat kan/wordt er gedaan worden tegen zulke mogelijke aanvallen?
      a. Naar specifieke policy documenten/beleidslijnen vragen (kopieën
         beschikbaar?)
      b. Oefeningen? Zie a.
      c. Is er een indeling welke volgens jullie het meest mogelijk zijn? Het is een
         combinatie van.

5. Wie zou u aanraden waar ik nog meer op gesprek zou moeten gaan aangaande dit
   onderwerp?

Hoofdvraag
To what extent is the terrorist threat directed at watersystems in the Netherlands realistic, is it identified by
the authorities and which measures are taken against these threats?

Deelvragen
   (i)   To what extent are Dutch water systems vulnerable to terrorist attacks?
   (ii)   In theory, to which extent can a terrorist attack targeting water systems take place and be
            succesfull?
   (iii)   If the threat is real, is it recognised and what measures are taken into account?

Attachment II

Coding book (In Dutch)

Family code 1. Structuuraspecten

1a. Organisatiestructuur
De plaats van de persoon die geinterviewd wordt binnen de betreffende organisatie

1b. Media
Hieronder vallen alle vermeldingen aangaande de media.

1c. Verantwoordelijkheden van de organisatie
Hierbij vallen alle vermeldingen aangaande verantwoordelijkheden die de geinterviewde partij heeft.

Family code 2. Procesaspecten

2a. Verantwoordelijkheden van de organisatie.
Wat zijn de grenzen van de verantwoordelijkheden van de organisatie.
De taken die de organisatie uitvoert.

2b. Verantwoordelijkheden van de overheid
Hieronder vallen alle vermeldingen van de overheid

2c. Opbouw van systemen
Dit zijn veiligheidssystemem
Dit zijn theoretische systemen

2d. Baten en Kosten
De overweging tussen voorbereidingen treffen tegen terrorisme, t.o.v. de kosten

Family code 3. Terrorisme

3a. Terroristische aanvallen
Referenties van/naar terroristische aanvallen

3b. Water terrorisme
Referenties van/naar terroristische aanvallen gericht op de watersector

3c. Vitale infrastructuur
Referenties van/naar vitale infrastructurele zaken

3e. Vormen van aanval

(i)   Hieronder valt het opblazen van watersystemen

(ii)   Hieronder valt het vergiftegen of het uit werking stellen van water zelve

(iii)   Hieronder van het hacken van bepaalde systemen

3f. Andere vormen van aanval

Hieronder valt niet terrorisme, maar een boze medewerker of een gek etc.

Family code 4. Mogelijkheid tot drijging

4a. Aantrekkelijkheid van 'water systeem' aanvallen

Is het wel aantrekkelijk om nederland aan te vallen? (resources, knowledge and impact, both in number of casualties as in psychological effects).

Zou dit ook gebeuren in de sector water?

4b. Security measurements

Elke referentie naar al bestaande security measurements of te implementeren.

Family code 5. Wat er tegen gedaan wordt

5a. Oefeningen

Hier wordt alleen de oefening gemeld. Verder geen voorbeelden of wat dan ook.

5b. Oefeningen voorbeelden

Hieronder worden verschillende scenarios geplaatst, voorbeelden voor oefeningen

5c. Beleid

Reeds gemaakt beleid om aanvallen tegen te gaan

5d. Security Measurements

Enige dubbele, wat wordt er tegen gedaan

5e. Organisatie houd iets achter

Wanneer betreffende organisatie iets achter houd

5f. Gevoelige informatie

Wanneer betreffende organisatie gevoelige informatie vermeld