WHY
THE WATER DISTRIBUTION NETWORK SHOULD BE CONSIDIERED CRITICAL INFRASTRUCTURE

Sergio Bianchi* Rosella Bolis**, Chiara Dell'Orto'', Emilio Lanfranchi^^, Andrea Zaccone**
with the contribution of Alessandra Lafranconi^ (health effects)

*Agenfor Italia - ** Lombardy Region - '' Lombardy Foundation for the Environment -
^^ Metropolitana Milanese – ^MD M.Sc. Environmental Health

EUROPEAN COMMISSION
Directorate General Home Affairs
Directorate A: Internal Security

PROGRAMME
Prevention, preparedness and consequence management of terrorism and other security related risks

AGREEMENT NUMBER
HOME/2011/CIPS/AG/400002108
ABAC NUMBER
30-CE-0488228/00-75

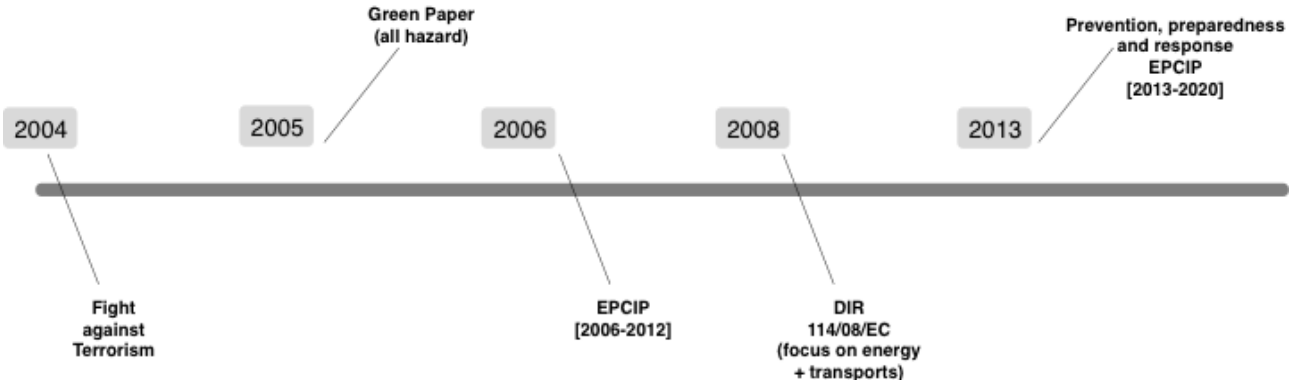
Index

Introduction

On the 12th December 2006, the EC presented a proposal for a directive on the identification and designation of European Critical Infrastructures (ECI) defining critical infrastructure as:

The physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States.

Since then, a complex and articulate debate has been launched on the definition of critical infrastructure, which lasted several years until the 2013-2020 EPCIP Directive.



With Directve No. 114 of 2008, the EU formally excluded water infrastructure from the category of critical infrastructure. The new definition of critical infrastructure incoporated the previous definition of 2006 within a new concept: "'*critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as result of the failure to maintain those functions."*

In fact, only two sectors enter the scope of the new definition of 'critical infrasturcture': energy and transport.

Water management is indeed a complex process in modern societies, and has an impact on many aspects of civil life, interrelating economic aspects with those of health, information management and wellbeing.

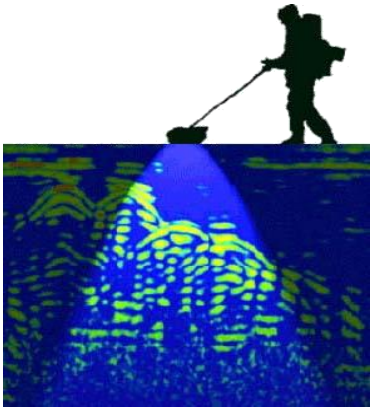
Water is channelled from immense resevoirs into infrastructure that transports it into lifting and treament plants before reaching the complex distribution networks that supply our houses, our offices, and our lives. These are all essentical aspects of civil life. With this research, and above all with the Milan simulation test, we hereby demonstrate beyond all doubt that water distribution infrastructure is a fundamental asset for the maintenance of vital social funtions, which if compromised would have dramatic effects on the vital functions of the system, the health of citizens, their safety and their economic and social wellbeing. Therefore, this infrasturcture is cricical, perhaps even more so than the energy and tranport networks.

(Map of the water cycle, Hera 2012)

The growing complexity of network management, summarized by this map of the water cycle, clearly shows that the protection of this strategic resource is in iteself a very complex matter. In fact, this system has many vulnerabilities, which are vastly spread across the territory.

This complex system multiplies types of threat, as we shall see.

There is also a growing informational technology component, of data production and management, which must also be considered as a new emerging factor in the overall analysis of threats by both water service operators and decision makers at large.



In fact, all major European water utilities, municipalities and operators now have highly structured informtaion systems to produce network data and use it for their own purposes and for external parties, as well as for the management of the water cycle through the remote control of various functions, not least water purification.

The creation of data regarding the networks allows the operators to have much more detailled information on the underground infrastructure, but this involves a management process for data contained in a complex management chain, with increasing vulnerabilities.

From **catchment** to **purification**, including the set of physical and chemical treatments required to make the water suitable for human consumption, up to the distribution through networks and the final phase of treatment, the entire water cycle is now subject to computerized processes that are contstantly increasing in terms of quantity, materiality and importance.

Chlorination plant of Milan S.Siro, Italy.
The system is remote controlled (Photo Agenfor Media 2013)

Therefore, the information technology factor, taken as a whole, today adds a new element of assessment with regard to the operational procedures of the water cycle, including the analysis of overall risk. Operators are aware that the quality and quantity of the water supplied to their citizens depends more and more on automated processes that remotely transmit information via cables, in some cases owned thereby but more often managed by specialized companies, not always internal to the operators themselves. Moreover, this information is stored in virtual spaces, often by parties external to the actual water cycle.

In particularly critical moments, the supply of the resource itself can depend on such information. Therefore, the 'cyber' aspect is an assessment factor that did not even exist until a few years ago, but that is now becoming increasingly important, as the quality of information and computerized management processes gradually grow and as the stakeholders involed gradually multiply.

1. THE MANIFOLD THREAT PROFILES

Because of its strategic nature, water has always been a target for those considered to be a threat. History is full of examples, dating back to 2400 BC when during the Sumerian era the kings of Lagash (now Tell al-Hiba, Iraq) diverted channels between the Tigris and the Euphrates to leave their opponents of Umma dry and force them to surrender. And only to continue with fighting between Peshmerga forces and Da'ish insurgents and around the dam of Mosul, Iraq, in the summer of 2014.

In Greek history, chronicles remember the actions of Solon in 600 BC who, as he laid seige to the city of Chrysó, poisened its wells with roots. Its citizens fell violently ill and as a result the city fell into the hand of the Athenians.

The list of conflicts over water is infinite: it extends around the world[1] and thoughout all ages. The types of conflict have been classified by various scholars under different typologies according to the reasons, *modus operandi* and objectives set by the various actors behind their actions. Further on, we will actually see that this type of threat analysis, which for the sake of brevity we will define as 'traditional', today is no longer able to capture the complexity of the risk analysis. First of all, this helps us in any case to understand the manifold profiles of what is defined as the '*modus operandi*' of the threat. Glieck defines 6 profiles:

[1] Gleick, P.H. 1994. "Water, war, and peace in the Middle East." *Environment* Vol. 36, No. 3, pp.6-on. Heldref Publishers, Washington.; Gleick, P.H. 1998. "Water and conflict." In P.H. Gleick, *The World's Water 1998-1999*, Island Press, Washington, D.C. pp. 105-135.

- **Control of water resources** by state or non-state actors. These are cases in which the supply of water or access to water represents the cause of conflict.

1958	Egypt, Sudan	Egypt sends an unsuccessful military expedition into disputed territory amidst pending negotiations over the Nile waters, Sudanese general elections, and an Egyptian vote on Sudan-Egypt unification; Nile Water Treaty signed when pro-Egyptian government elected in Sudan.

- **Military instrument** (state actors), when water resources or infrastructure are used by a nation or State as a weapon during war operations.

1967–1972	Vietnam, United States	The US military, in "Operation Popeye," uses silver iodide for cloud seeding over Indochina (Vietnam), in an attempt to extend the monsoon season and stop the flow of materiel along Ho Chi Minh trail. "Continuous rainfall was intended to slow down the truck traffic and was relatively successful."
2012	Libya	During the 2011 Libyan Civil War, forces loyal to dictator Muammar Gaddafi gain control of a water operations center and cut off water supply to the capital. The system controls Libya's Great Manmade River—a system of pumps, pipes, and canals that brings water from distant aquifers to Tripoli and other cities. Half the country is left without running water, prompting the UN and neighboring countries to mobilize tanker ships to deliver water to coastal cities.

- **Political instrument** (state and non-state actors), when water resourses and infrastructure become a political means.

2009	North Korea, South Korea	Without previous warning, North Korea releases 40 million m^3 of water from the Hwanggag dam, causing a flash flood on the Imjin River. In South Korea, at least 6 fisherman and campers are drowned. North Korea claims that the water had to be urgently released and promises to warn the South of future releases. South Korea fears that North Korea could use the water of the dam as a weapon during a violent conflict.
1999	Kosovo	Serbian engineers shut down water system in Pristina prior to occupation by NATO.

- **Terrorism** (state and non-state actors), when water resourses and infrastructure are used to generate mass terror among the civilian population in order to achieve political or strategic objectives.

2001	Philippines	The militant Islamist separatist group Abu Sayyaf threatens to poison the water supply in Isablela, a mainly Christian town on Basilan island in the country's south. In October, residents in six nearby villages suspected contamination due to water that smelled like gasoline. Local officials responded by closing pipelines and bringing in drinking water by truck. In the months following the 9/11 attacks on New York, numerous false alarms of terrorist activity are reported around the world.

- **Military target** (state and non-state actors), when water resourses or infrastructure become the target of military operations.

1941	USSR and Germany	The strategically-important Dnieper hydropower plant in the Ukraine is targeted by both Soviet and German troops during WW II. On August 18, 1941, the dam and power plant

	are dynamited by Soviet troops retreating in front of advancing German forces. The facility is bombed again in 1943 by retreating German troops.

- **Development dispute** (state and non-state actors), when water resourses or infrastructure become the source of conflict in economic, community and social contexts related to the development of an area or region.

2001	Pokomo farmers and Orma cattle herders	At least 130 people are killed in a string of clashes between Pokomo farmers and Orma, semi-nomadic cattle herders over access to land and river water.

Ethiopian Oromia and Somali Regions	Ethiopian Somalis attack a Borana community in the Oromia region over ownership of a new borehole being drilled on the disputed border between them. Three people from the Oromia village of Kafa are killed and seven injured, and the entire community driven from their homes. The drilling rig is destroyed, as well.

As is known, there are at least 100 different classifications of what "terrorism" is from a theoretical standpoint. Its definition is a much-debated topic on a European and Western level[2]. We will not explore this subject herein, limiting ourselves to refer to the CIPS directives of the EU[3] as part of the broader Security and Safeguarding Liberties programme, which addresses the matter with a very pragmatic approach.

The analysis of the events classified as terrorism that arise from ANNEX 1 highlights, however, some very useful aspects for the purposes of our research and the related field tests.

Indeed, the first finding that emerges from the analysis of the time series is that it is not easy to carry out terrorist attacks on the water supply or its reservoirs.

This is probably the main reason why the number of victims reported in the time series is relatively low compared to other incidents of terrorism. On the other hand, we have to admit that if we were to examine the time series of attacks on skyscrapers before 9/11, we would probably find a similar result. Therefore, the number of victims or recurrence of the act alone may not be irrespectively considered indicators of system security, contrary to what is claimed by the most common metric analyses.

Moreover, the example of the Twin Towers is also interesting for another reason: even the best risk assessment processes conducted using the widest range of methodologies and technologies tend to fail if they only follow historical examples. We have to admit that modern terrorists and insurgents, using planes or pressure cookers as new instruments to attack the most unexpected aspects of our daily lives and spreading terror for the purpose of exerting forms of control, have shown a perverse imagination that is often difficult to foresee.

The second finding that emerges is the apparent discontinuity and geographic disproportionality of the phenomenon, which seems to be much more extensive, for example, in North America

2 Alex Schmid, Terrorism – The definition problem, in Case Western Reserve Journal of International Law, 36 (2), 2004. The Change Institute, Studies into Violent Radicalisation. The Beliefs Ideologies and Narratives, Brussels, DG JFS 2008 pg 19. La UE (Council Framework Decision on Combating Terrorism, 2002/475/JHA, 13/06/2002), in line with the High Level Panel of the United.
Alain de Benoit, Terrorismo e Guerre Giuste, Napoli, Guida, 2007 Nations (A/59/565 2004) defines terrorism as "an international act which may seriously damage a country or an international organisation, committed with the aim of seriously intimidating a population, unduly compelling a Government or an international organisation to perform or abstain from performing any act, seriously destabilizing or destroying fundamental political, constitutional, economic or social structures by means of attacks upon a person's life, attacks upon the physical integrity of a person, kidnapping, hostage-taking, seizure of aircraft or ships, or the manufacture, possession or transport of weapons or explosives."

3 On 12 February 2007 the Council of the European Union adopted the legal basis for both Programmes: Decision 2007/124/EC, Euratom1, establishing the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" (CIPS Programme) and Decision 2007/125/JHA2 establishing the Specific Programme "Prevention of and Fight against Crime" (ISEC Programme) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

compared to other parts of the world. The evidence tells us that this is not so. In fact, methodological updates are also required for this aspect, since the time series poses the problem of reporting, which appears to be extremely uneven from one geographic region to another and should not be used as an indicator of the threat level or for risk analysis.

Predicting the unpredictable on the basis of feeble evidence and entering into the logic of a potential terrorist has been the task of our working group, which presented itself as a creative test in order to assess the strength and resilience of our water systems and impact of a potential attack on the civil life of a city such as Milan. Given the nature of the threat and the availability of open source information, instead of using metric tools, we based our risk assessment on theatre analysis.

2. AN EMERGING THREAT: HOMEGROWN ENVIRONMENTAL TERRORISM

A careful reading of the various events shows two models of terrorist threat, clearly distinct from one another and very marked:

A) A traditional model of terrorism, which is in some way predictable using the traditional methods of risk and threat assessment and

B) A model closer to the processes of 'homegrown terrorism', which is difficult to predict using the traditional instruments of risk assessment.

Let us now take a closer look at the two models applied to the time series list:

First of all, it is evident that the major forms of threat, until now, have focused on the physical infrastructure of water.

Attacks on dams, pipelines and power plants are some of the recurring elements of both terrorist groups operating at various latitudes and under various names, as well as of incidents of a technical nature. This type of threat is extremely significant, as it may cause high numbers of casualties, as demonstrated by the tragic accident of the Vajont in Italy on 9 October 1963, which caused 1,917 casualties. Beyond the aims or intent (accidents or terrorism or a combination thereof) this area of infrastructure, by its very nature and technical dimensions, is linked to *modus operandi* that are much more suited to classic models of terrorism. In fact, if we analyse the existing reports, we may note that these types of attacks are carried out by radical movements of various kinds (FARC, Tamil, Taliban, KLF, Abu Sayyaf, the PKK, Hezbollah, etc.), which operate using classic group formations, according to the insurgency model, use of explosives and military-style action. They usually have the purpose of asserting the control of an opposition group over assets (water, infrastructure, populations, etc.) that are typically under the control of certain government authorities. That is to say that the primary objective of this operative model, which we incorrectly classify under the term "terrorism", is to challenge the authority and sovereignty of a government, launching a claim against the State through terror and war. These are the actions that occur most frequently in the time series, causing the greatest damage and casualties.

Against this traditional "terrorist" approach (which would in truth be more correct to call 'insurgent'), much has been done over the years by various governments in terms of the physical

security (video cameras, networks, surveillance systems, early warning, military response, as in the case of Da'ish, etc.) of reservoirs on a European and global level, the tracking and profiling of terrorist movements and prevention and counter measures. This type of threat, as deadly as it may be, seems to be well considered by the operators of water systems and their security agencies. Consequently, the level of response is already high.

A less obvious second type of threat, however, is represented by cyberattacks.

Possibly the most striking case of this kind occurred in Queensland (Australia) in 2000, when the local police arrested a computer technician who, using a computer and a radio transmitter, attempted to take control of the treatment plant to spread waste water through parks and towns and infect the population with E. coli. According to the American FBI, Al-Qaeda has supposedly tried to obtain information concerning to the management of water systems on numerous occasions.[4]

Although reporting techniques are unfortunately not systematic and therefore the metric and quantitative analyses tend to be inaccurate, we know that cyber threat is an essential component of risk analysis if you want to properly profile the threat. Bruce McCormack, an Irish expert on water supply, reminds us[5] that Ireland was subjected to a 'White Hut' simulated attack, when a foreign government took control of the SCADA system of a Irish county, who then warned the Irish Government so as to highlight the vulnerabilities of the system.

In 2011, Russian cyber hackers attacked the pumping system in Springfield, Illinois (USA) using stolen SCADA credentials managed by the software provider. In 2012, serious destructive attacks against information systems in the Gulf destroyed 30,000 hard drives of Saudi Aramko and, in Qatar, dealt a blow to the operating system of Ras Gas.

The growing importance of the cyber threat, intended as a specific *modus operandi*, is closely linked to risk analysis in its most correct form and it demonstrates the weakness of analyses based on segmented concepts such as ‘terrorism’, ‘insurgency’, incidents, etc. Subsequently, they also show the weakness of ‘anti’ policies (anti-terrorism, anti-insurgency, etc.).

The cyber threat is increasing since the area of conflict tends to extend beyond the physical theatres (land, sea, air) to new spaces where the exertion of control marks a competitive advantage for whoever wishes to violate the sovereignty of other actors. In the past, the sovereignty of a government was based on the control of a State, in terms of its tangible dimension of people/nation (tangible and intangible) with its land, sea and air territory. Today, these spaces have been widened because States, such as in the case of Ireland, may have their tangible and intangible sovereignty violated without there being physical occupation/violation of the tradition theatres of land, sea and air. Internet, satellite networks and global communications represent a new dimension of the theatre where the competition for the control over certain resources takes place, which is the basis of internal and external conflicts, or a combination of both.

[4] http://www.ionizers.org/water-terrorism.html
[5] Dialog with Bruce McCormack, summer 2014, Lubijana (Slovenia).

Not only that: access to information regarding water systems represents a modern form of functional monitoring of the planning and carrying out of attacks of any kind. If in the complexity of the water network, malicious competitors wish to measure the effectiveness of their actions in terms of damage, they no longer have to station themselves in some vehicle near the target to register the movements of the victim, as is the case with traditional terrorist ambushes. Instead, they merely require access to a database that informs them of flows and water consumption, pressure, the position of hydrants and valves that supply a certain system, for example, so as to accurately choose the location to attack a specific target from. Paradoxically, at a European level this information is rarely protected and indeed in many cases the institutions involved in the governance of the system promote the accessibility and usability thereof for technical and economic reasons of various kinds, not least the provisions of the EU Directive INSPIRE.

This type of cyber threat is relatively new as it uses innovative, more modern *modus operandi,* is growing in character, is exactly half-way between traditional models and those homegrown and, in conjunction with other factors, plays a central role in the risk analysis and field testing we conducted.

In fact, these attacks can be carried out both by structured movements with complex logistics, as well as by single solitary actors with the necessary skills, and even by individuals with the most diverse personal motivations, as the Queensland case would indicate.

A third type of threat, less frequent in the list of historical events, it is instead linked to the possibility of contamination of the water cycle.

Different profiles of this type of threat emerge from the time series, which vary in terms of *modus operandi* as well as the objectives of the actors. As in the case of cyber attacks, this type of bioterrorism may occur in classic forms of terrorism or in homegrown forms, and in the latter sense has attracted the attention of theorists of Al-Qaeda and its network. This may be the work of those who today we love to define solitary actors or lone wolves, or of movements with complex organization, and can manifest itself in the form of a physical attack on the network or be combined with the aid of information systems via software such as ‘shodan’ or via access to operator databases using various methods. What makes the difference, in terms of operating mode, between this model and the complementary model of cyber attacks is that in the former case, the malicious control is exerted through cyber intrusion, which aims to alter the functional parameters of the networks, to remotely take control or disable them. In this case, however, it is necessary to have access to the physical network, involving the intrusion and the introduction of harmful substances capable of causing physical damage to users. Therefore, cyber attacks can easily be combined with malicious forms of network intrusion, with the aim of causing a damaging domino effect. In the latter case, the quantification of the damage is essentially different since it affects not only the victim company, as with cyber attacks, but also citizens and the entire social system (hospitals, civil defence, security, politics, etc.). The combination of these *modus operandi* currently represents the greatest threat to water distribution systems, as we shall soon see.

State terrorism or rogue states

Another way to classify threat in traditional risk analysis is based on the profile of the actors.

The time series show types of threats related to State terrorism, both in classic forms and in the more recent methods of rouge or failed States, within which organized terrorist groups, even by proxy, may gain access to the production of weapons of mass destruction.

These types of threats intend to use extremely dangerous pollutants that are, however, difficult to find, which only a state or military or state-sponsored (proxy) terrorist organization may have access to in large enough amounts to create panic or mass casualties.

The technical charts of these products, often available as open source, as well as the debate within the global intelligence community, highlight the fact that there are biological and chemical threats of major importance due to their degree of hazard and behaviour in aquatic environments. But it is evident that products such as nerve agents (such as sarin), pathogens (such as anthrax or cholera), toxins (such as Botox), pollutants such as BZ or radioactive products are available in large enough amounts to attack the water distribution network or water catchment areas, only to the extent that a state produces them, since they are not easily available on the market or in nature. Moreover, to make these substances effective, a high level of knowledge is required to have the necessary skills to know how to pollute the network with suitable substances, taking into consideration the chlorination process, pressure, the complex nature of the networks and, above all, the flow.

The corresponding logistics, treatment and importation are very complex.

Homegrown environmental terrorism

Here a very specific threat profile emerges, which we could define as ‘homegrown environmental terrorism’, namely with the objective of causing extensive damage to the water system, however with commonly used products and instruments that are a part of our daily lives, by agents or terrorists that are difficult to identity since they are ‘lone wolves’ or ‘self-radicalized’.

There are many examples of these models of homegrown terrorism, i.e. spontaneous and often indigenous, and there is vast literature available on the subject.

This threat has a substantially different profile compared to those examined so far since it requires very light logistics and above all the selection of readily available contaminants that are relatively easy to use also by individuals and groups who do not have specialist knowledge and skills.

Some of these products are used in large quantities by commercial companies in Europe and are distributed either freely or with technical restrictions (e.g. phytosanitary licenses) that are unrelated to security classifications.

Products such as some commercial pesticides or their active ingredients can have very serious effects on humans if ingested and introduced into the water system. Other non-organic chemicals,

such as arsenic or the derivatives of the hydrocyanic family are soluble and lethal, as pointed out by Hickman[6] in the case of NaCN for small water circuits (at a building level, for example).

Not to mention the potential risk associated with the acquisition of deadly pollutants from petty criminals operating in minor crime (such as the theft of metals) and working in conjunction with forms of organized crime to carry out environmental crimes[7]. Perhaps for the purposes of general threat analysis and understanding the interoperability of systems and therefore their vulnerability, the fact that in specific cases simple copper theft has disabled, for example, strategic military installations should not be underestimated. Similarly, recent blackouts have caused the collapse of the water system in entire inner city areas, causing understandable panic among citizens and blocking all other parallel networks, with very serious downstream effects.

3. WHAT WE SEE DEPENDS LARGELY ON WHAT WE WANT TO SEE

The traditional differences between natural, anthropogenic or technological disasters, or between different actors, which still form the basis of security analysis in the infrastructure sector, are clearly inadequate for capturing the profile of this new, changing threat, which is internal and external at the same time and draws its strength from domino effects, while maintaining a certain profile related to the reasons or intentions behind the behaviour. The traditional models of threat analysis, based on the probability, frequency and severity of terrorist acts, measured by improbable metric risk matrices, are at the danger of becoming merely theoretical exercises in relation to manifold threats such as these, which instead are mobile and can make use of a wide variety of tactics depending on the damage they wish to cause.

It is impossible not to see that behind and within many of these traditional analyses there is some confusion between *modus operandi*, the type of actor and the nature of the threat, which makes it very difficult to conduct proper risk analyses. Furthermore, by depending exclusively on 'intentional' models that differentiate between types of risks on the basis of the assumed intention of certain actors, there is a greater risk of being misled with respect to the specific nature of the threat, which is always represented by an attempt to take control and the desire to create a specific type of damage, often uncontrollable and separate from intentionality, as a statement of power.

Instead of using the traditional metric instruments of risk assessment, we applied a method that for the sake of simplicity we will call the 'What if' methodology, in other words a scenario analysis. We put ourselves in the shoes of individuals wishing to carry out attacks for any number of reasons. We attempted to see the unseen, to reason with the mind of those who find themselves outside the system and want to cause damage, trying to measure the extent of the damage and even its unintentional effects, i.e. on the chain systems typical of the analyses carried out in case of accidents.

[6] Hickman, D. C. (1999). Chemical and Biological Warfare Threat: USAF Water Systems at Risk. Future Warfare Series No. 3. Air University, US Air Force Counterproliferation Center, Maxwell AFB, Alabama, p. 36, online at http://www.au.af.mil/au/awc/awcgate/cpc-pubs/hickman.htm.
[7] Quest'area di analisi è oggetto della ricerca che Agenfor conduce con Europol e SOCTA nell'ambito del furto di metalli con il progetto PolPRIMETT II http://www.pol-primett.org/

By changing perspective, we were able to test the resistance of the networks, but more importantly, anticipate and prevent attack patterns that are generally considered unpredictable. Precisely, 'What if…'

Before the Boston Marathon, no one imagined that a pressure cooker could be transformed into a weapon for an attack. Neither the metric analyses nor the various models of risk assessment had ever considered the operative dimension of the threat before the marathon, just as up until 9/11 a scheduled flight could hardly be considered a weapon. Yet this is precisely what characterises this manifold and often unpredictable threat profile.

Therefore, our work was organized around a detailed analysis of the models, in an attempt to:

1- identify the most vulnerable elements of the water system in relation to the type of risk, segmenting the intensity of damage based on complexity, regardless of causality or intentionality;
2- identify the potential technical means that could be used by the various profiles of the aforementioned actors (the traditional model and homegrown environmental model);
3- assess the role of information technology and the new cyber profiles both in terms of potential terrorist acts and as a supporting member;
4- finally, build an analytical model based on the real test, 'What if...'

We quickly realized that traditional models of the schematic division of risk, based on intention, do not work in the case of the environmental homegrown threat. In the risk analysis of these types of threats, damage to persons, processes, infrastructure or reputation is not determined by terrorism, an accident or a technological flaw. These categories may not be segmented or divided, but rather may operate together within the same threat, regardless of whether or not it was planned by those seeking to cause damage.

The confusion in the analysis stems from the fact that often the concepts are reversed and the *modus operandi* becomes the threat. Terrorism is not a threat, but the *modus operandi* of those who wish to spread terror among the civilian population, that is those who wish to cause damage in order to establish their own form of competitive control. The threat consists in what underlies the *modus operandi,* for example extreme political competition, a clash between countries but also limited social conflict that may be exploited by broader movements (think locally, act globally) or even a simple individual labour dispute or personal grievance. The exact definition of the threat, taken as a whole, determines the degree of risk and subsequently the prediction of damage, in the knowledge that a single threat may simultaneously use multiple operative modes (from terrorism, to protest, all the way to insurgency, for example). Threat analysis is what determines the assessment of the potential damage, with all that is then necessary in terms of prevention and response. Accidents, deliberate attacks and technologies may become mixed up in events that often transcend the original intentions of those wishing to cause the damage and that are highly probably given the ease with which the existing barriers blocking access to information and instruments can be overcome and due to the interconnected nature of infrastructure and systems in modern societies.

This emerging threat is much more difficult to study and profile since the reasons (or grievances) may be extremely flexible and go from being nationalistic, to religious, eco-terrorist (which is a different concept from that of environmental terrorism described herein), political, or

even purely personal reasons with relative ease. Or they may simply be mixed with different shades or alliances, temporary or lasting, consciously or not for the individual actors, such as in the case of the recruitment of 'insiders'. In addition, the damage does not only depend on the profile of who commits the act, since domino effects are often unpredictable within these complex systems. An employee (so-called 'insider') with personal complaints who decides to damage their company - a fact that could result in a low metric rating according to traditional models - may inadvertently cause extensive damage, possibly greater than that of a terrorist attack. It should not be forgotten that one of the hypotheses behind the biggest environmental disaster in history, in Bhopal, does not exclude this possibility.

The heart of the scenario analysis therefore revolves around the vulnerability of the system, regardless of the motives of those wishing to cause damage, for which is it is often impossible to accurately calculate the reach, since this depends on extremely complex factors.

(The area subject to attack)

In order to assess the vulnerability of the water system we formed an interdisciplinary team with few financial resources and little expertise - similar to the starting conditions of isolated individuals - but nevertheless in a position to simulate the carrying out of an attack in a central area of the city of Milan, one leading to the Expo platform. Incidentally, an attack on Expo, which has a circular and semi-closed system, would be far more deadly than one conducted on the area in question. Additionally, it should also be noted that events, especially in the case of large ones such as Expo 2015, are catalysts of the threat and therefore in these cases the systems of security design for water networks should be planned with particular care.

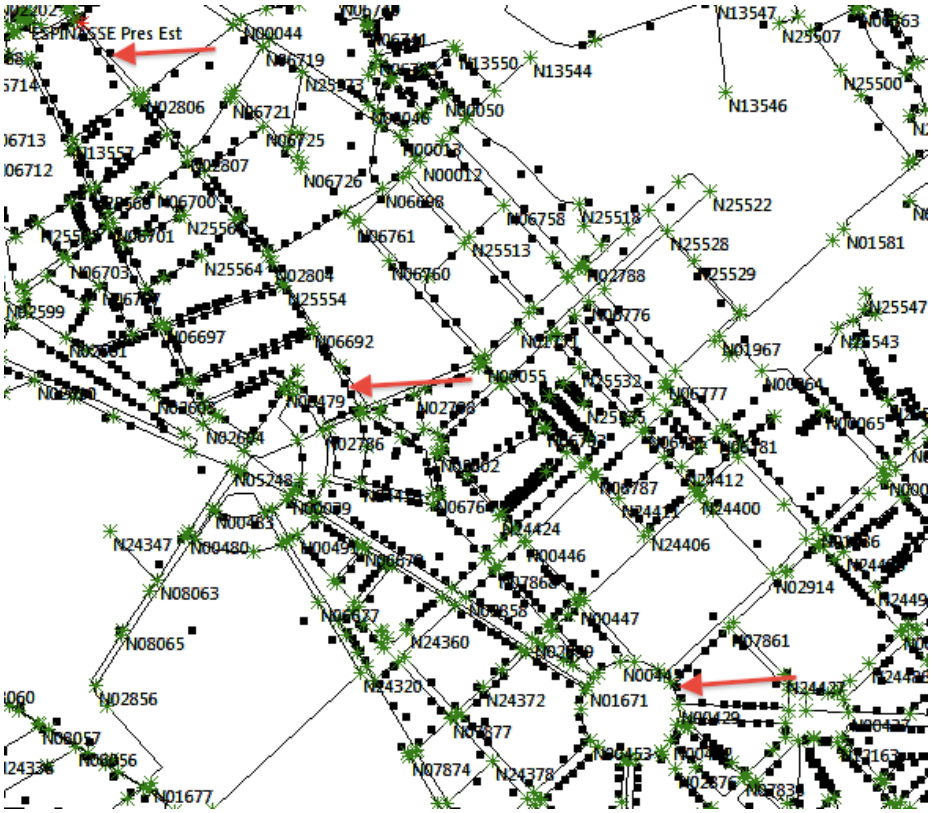
The outcome of the simulated attack produced a range of results or scenario analyses, which demonstrated the danger of the hypothesis. The scenarios were calibrated according to the times and the dilution of the substance in the water system, thus taking into consideration a complex set of parameters.

The attack was simulated down to the smallest detail, to the point of inspecting the streets as a small group of terrorists or insurgents might do; we carried out intrusions on the information system of the Lombardy Region, in order to understand how to direct the attack, and considered the most economical means in terms of pumps, tankers and the purchase of materials. Above all, we based our simulation of the attack on a limited time frame.

The result is dramatic and reveals in all its gravity that water infrastructure is absolutely critical, deserving much greater attention from the European Union, the national states and operators.

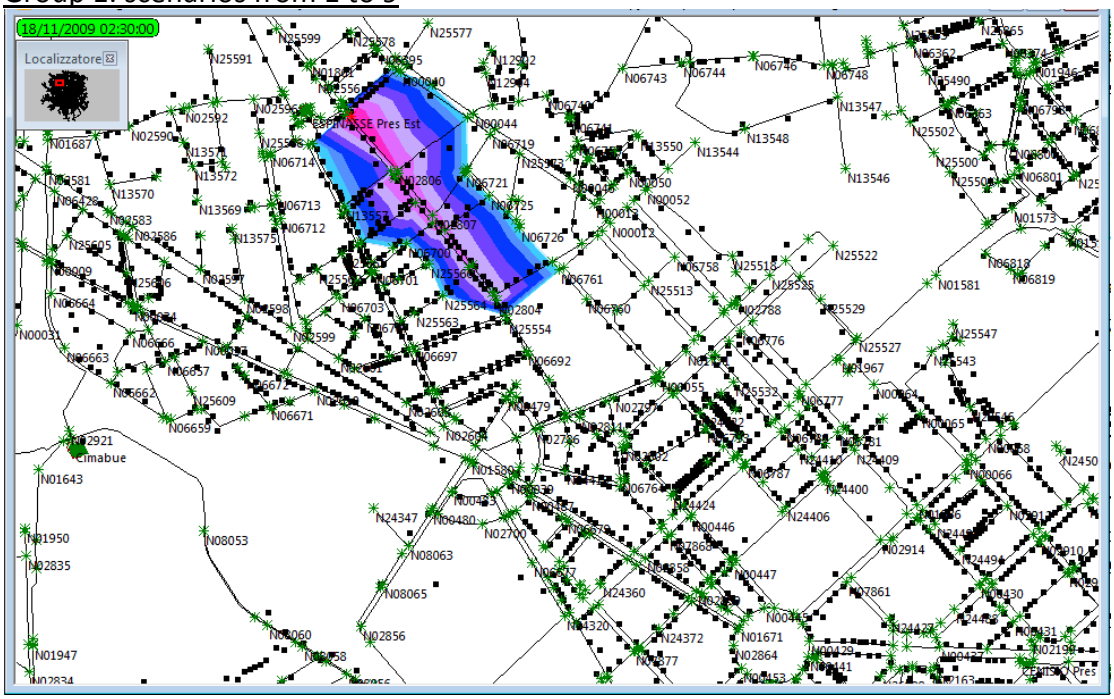
4 SCENARIOS

Health effects are described in 54 different scenarios, which are projected over different **day time** (N=night, that is the simulated attack of 2 am; D=day, that is the simulated attack of 6.30 am), different **time lag after the attack** (0.5=half an hour after the attack; 1=1 hour after the attack; 2=2 hours after the attack), different **distance from the injection point** (near: X = 1511079.16 Y= 5038643.65; middle: X = 1511649.32 Y= 5037853.2; far: X = 1512343.08 Y= 5037231.06, where the three points laid on the main-stream water pipeline, in a distance ranging from few meters to 2 kilometers from the injection point, as it is represented in the picture below), and different **exposure to contaminated water** (1=1 glass; 2=2 glasses; 3=3 glasses; where 1 glass of water = 200 ml). Health effects are assessed for human individuals of 70 kg of body weight, whose only exposure route is drinking water.



Health effects are presented for the following scenarios:

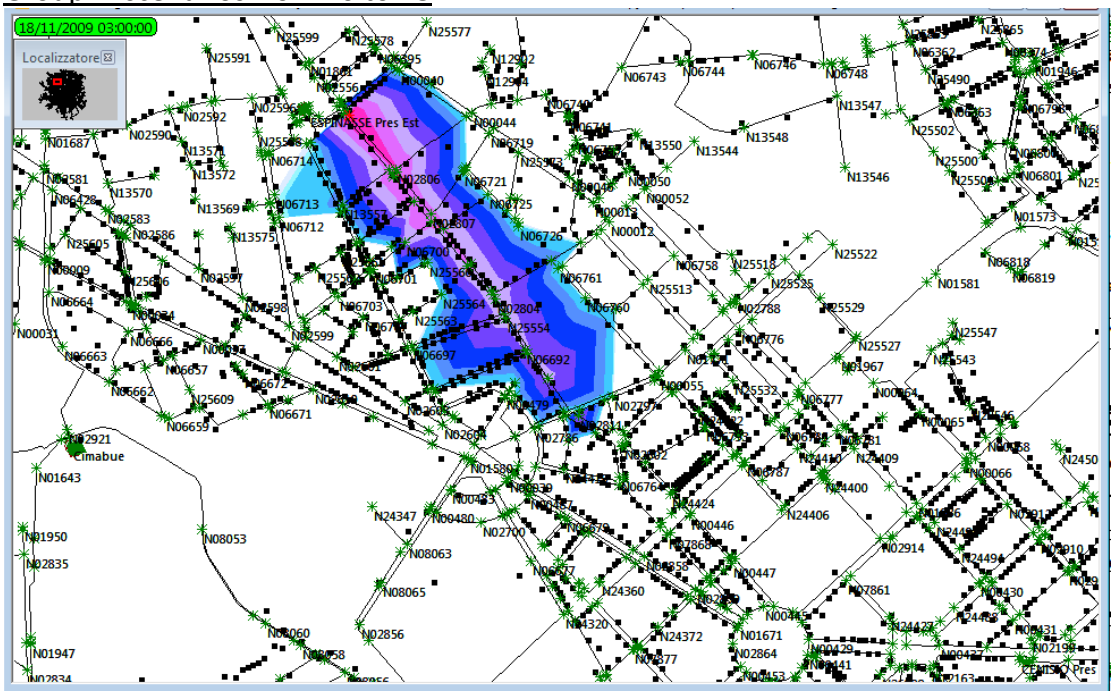
Group 1: scenarios from 1 to 9



In scenario 1, which considers human beings of 70 kg of body weight who drank 1 glass of contaminated water, roughly 1 gram of the pollutant would be introduced, resulting in an internal concentration of 1.56 mg/kg-bw for the commercial produc. This value is well above the LD_{50}, therefore theoretically we could assume that at least half the population would die, or, more realistically, suffer from very severe symptoms (it should be recalled that very few human deaths have been documented after ingestion of carbamates).

A higher number of affected people, and more severe symptoms, should be observed in scenarios 2 and 3, where the internal concentration rose to 3.11 and 4.67 mg/kg-bw.

Group 2: scenarios from 10 to 18

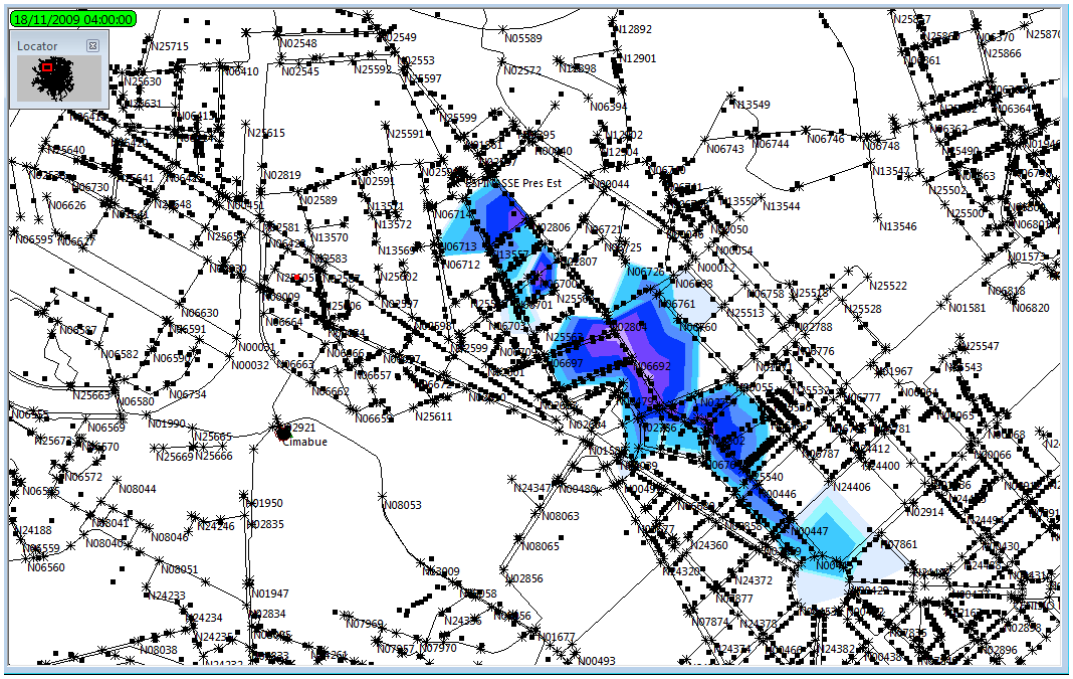


One hour after the night attack (3 am), at the first monitoring point, a concentration of 5-5.9 g/l has been detected, while at the second monitoring point the concentration decreased to 2-2.9 g/l, not yet reaching the third monitoring point.

In scenario 13, which considers human beings of 70 kg of body weight who drank 1 glass of contaminated water, roughly 0.5 gram of pollutant would be introduced, resulting in an internal concentration of the commercial product of 0.700 mg/kg-bw. Being the value above the LD_{50}, theoretically we could expect deaths or, more realistically, severe symptoms in at least half the exposed population (it should be recalled that very few human deaths have been documented after ingestion of carbamates).

Scenarios 14 and 15 are expected to affect a higher number of people, and to produce more severe symptoms with respect to scenario 13.

Group 3: scenarios from 19 to 27



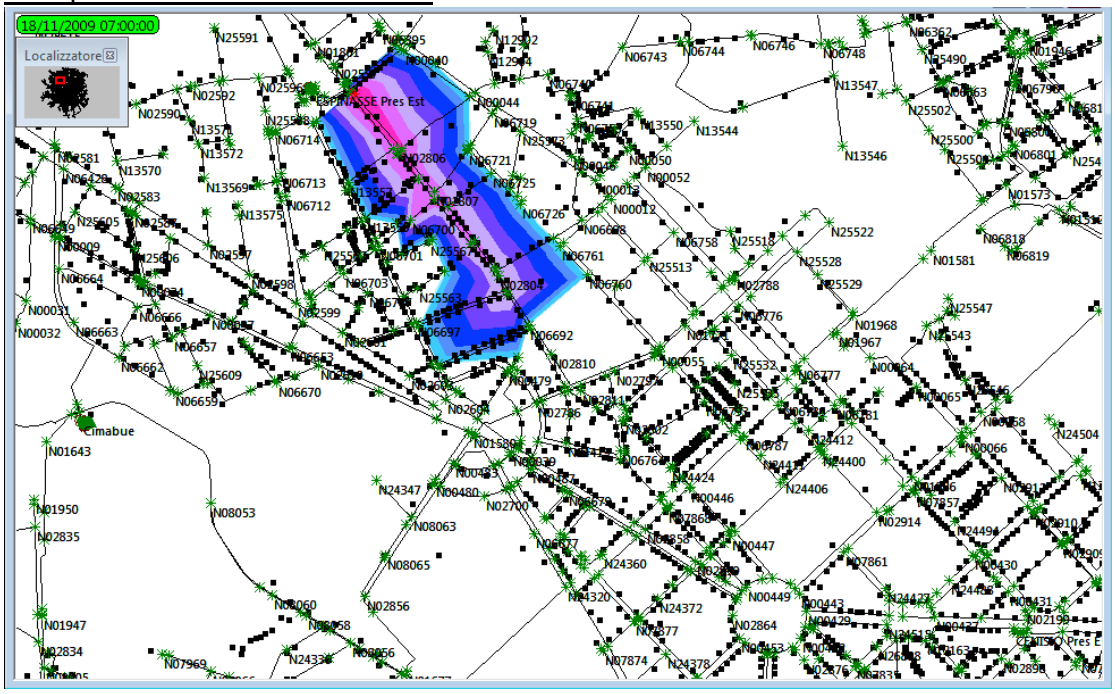
Two hours after the night attack (4 am), the estimated concentration was 0.5-1.4 g/l at the nearest point, 2-2.9 g/l at the middle point, and 0.05-0.1 g/l at the further point.

In scenario 19, which considers human beings of 70 kg of body weight who drank 1 glass of contaminated water, roughly 0.2 gram of the would pollutant be introduced, resulting in an internal concentration of the commercial product of 0.271 mg/kg-bw. We should expect surely less than half the exposed population to show very severe symptoms, and theoretically death, while a significant fraction of the exposed population will suffer of mild symptoms.

Scenarios 20 and 21, with internal concentration of 0.543 and 0.814 mg/kg-bw, could manifest more serious consequences, severely affecting more than half the exposed population.
In scenario 25, which considers human beings of 70 kg of body weight who drank 1 glass of contaminated water, roughly 15 milligram would be introduced, resulting in an internal

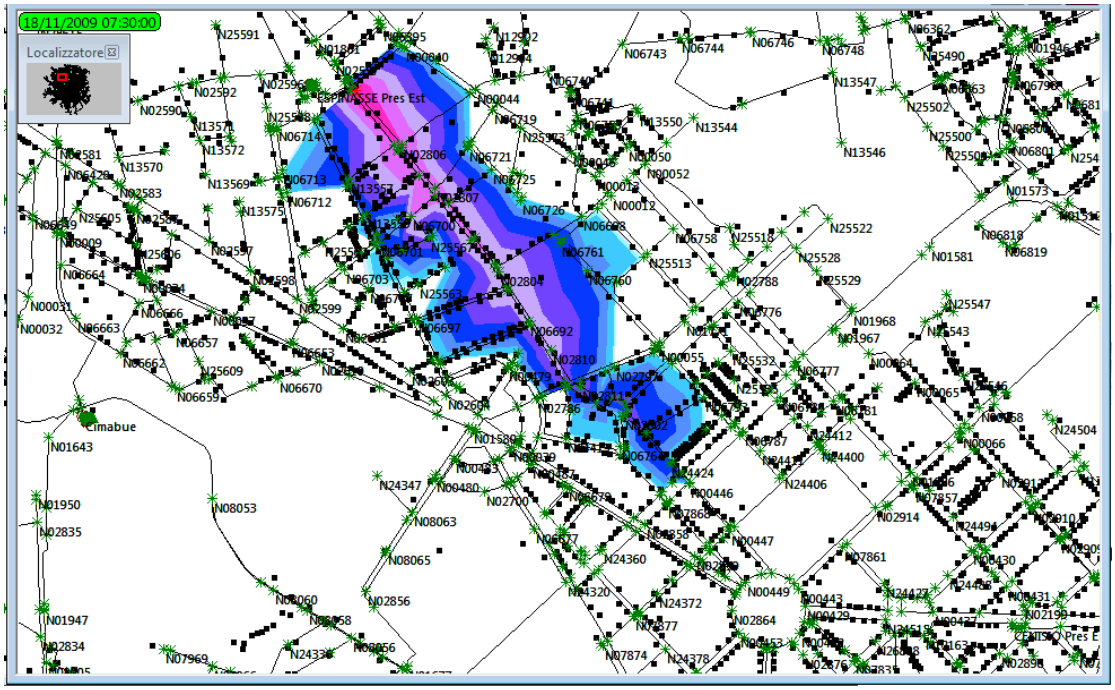
concentration of 0.021 mg/kg-bw. Very severe and mild symptoms should be manifested only in highly vulnerable individuals.
In scenarios 26 and 27, with 0.043 and 0.064 mg/kg-bw, we expect more frequent and slightly more severe symptoms, but no deaths.

Group 4: scenarios from 28 to 36



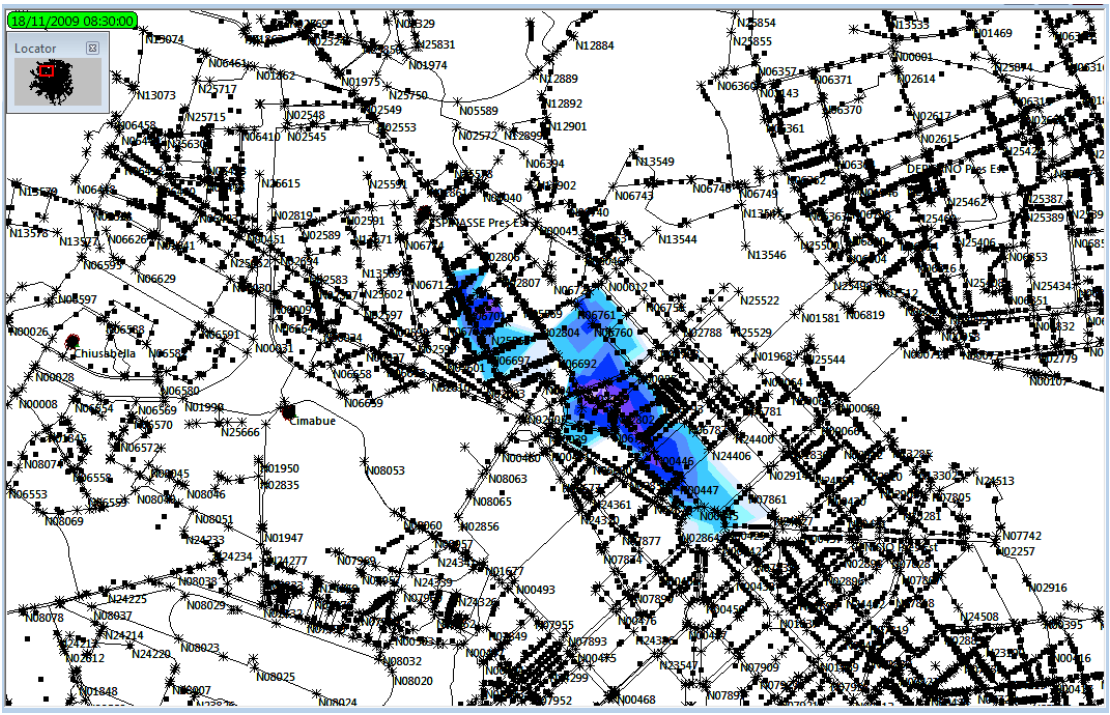
Half an hour after the morning attack (7am), in correspondence to the first monitoring point, the active pollutant has been found at a concentration of 5-5.9 g/l; no traces of the contaminant have been revealed downstream.
For scenarios 28, 29 and 30, the observations of scenarios 1, 2 and 3 are again proposed.

Group 5: scenarios from 37 to 45



One hour after the morning attack (7.30 am), there was no change in the estimated concentration at the nearest station to the injection site (5-5.9 g/l); the contaminant was found at the second station (3-3.9 g/l), but was drawn up before reaching the third station.

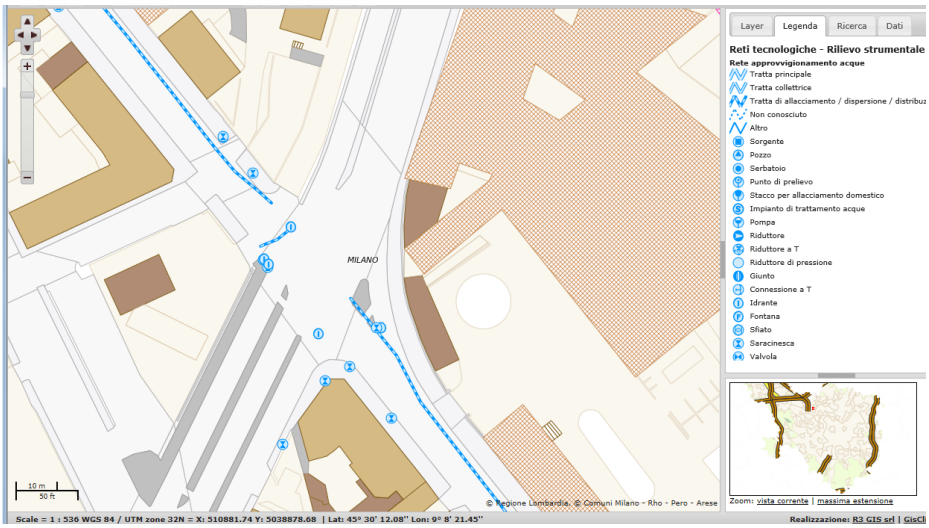
Group 6: scenarios from 46 to 54



pollutantOnly two hours after the morning attack (8.30 am), the was no longer present at the first monitoring point, while its concentration has been estimated as 0.5-1.4 g/l and 0.1-0.5 g/l at the second and third monitoring points, respectively.

All scenarios are schematically presented in Table 1, where three different levels of alert have been set: the more critical scenarios are those for which the substance internal concentration appeared higher than LD_{50}, intermediate scenarios are those for which the concentration was higher than LOAEL but lower than LD_{50}, and safe scenarios are those for which the concentration didn't reach the LOAEL.

In fact, we realized (and demonstrated with a field test) that the network is vulnerable in many places - dramatically vulnerable. Above all, the test carried out demonstrates the water catchment and distribution systems can have a domino effect on the vital assets of society, which can be simultaneously affected by multiple instruments (IT, physical, etc.) and with multiple contaminants, even simultaneously from several locations, thus making the identification of the threat extremely difficult for the purposes of an effective and rapid response.



(Potential access points to the water supply)

The *modus operandi* used by those who wish to cause damage has a high degree of scalability that is not necessarily dependant on the threat profile, although it certainly has a relationship with this: a small group of solitary actors with various grievances may indifferently carry out an attack in a central street of Milan, resulting in mass casualties, panic and extremely significant socio-economic damage with very few resources and little knowledge.

But exploiting the same points of vulnerability of the water system, the same group could also carry out a simultaneous and continuous attack from multiple locations (for example, by renting several apartments), operating within private residential property (and not from external road access, as is the case of our analysis-test), exponentially increasing the level of threat and damage, making both the identification and response actions far more complex. It is one thing to operate from a single location for a few hours outdoors with a tanker connected via road access and with limited amounts of material. It is likely that a good civil protection system would quickly raise the alarm, having an expected influx of patients with similar symptoms in hospitals or clinics, with emergency calls and alarms all originating from a single area. Quite different, however, is the case in which stocks of pollutants patiently collected over time in a garage or private deposits in multiple residential buildings positioned in different strategic locations throughout the city are available. From within ones own home, hidden from prying eyes, it would be much easier to carry out a continuous and lasting attack using the *modus operandi* defined by the exercise, massively polluting the water distribution network and causing mass casualties in multiple areas over a long period of time.

Yet the test also demonstrated that the flaws of the system are so great that with the same *modus operandi*, other threat profiles could produce risks and damage of a very different nature. Operations focused on specific targets are also possible, which often have a serious and life-threatening impact on those affected, but generally with limited numbers. Paradoxically, this is made possible thanks to the precision and the quantity of data available on the functioning of the network that may be found via the GIS or mapping information systems of various public and private stakeholders, often fragmented and uncoordinated as a whole. A technical request is all

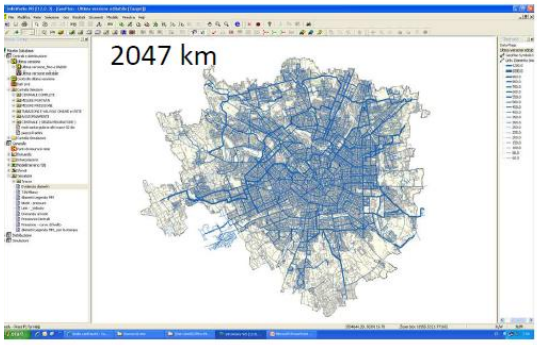
that is needed, unless one wants to hack into a private database, to obtain basic information on specific network segments in almost all European countries, with very few exceptions. With little effort and the slightest technical skills, it is possible to understand where the most vulnerable access points are located, the direction, the flow rate and pressure of water flows, as well as essential aspects of the management system or even systems, in the case of GPR readings. With this material resulting from a new simplified and administrative model of malicious surveillance, in the case of water distribution, attacks targeting barracks, prisons or military and political centres are conceivable, which become feasible through the exploitation of vulnerable aspects of the network that emerged during the exercise, even using the same logistics and materials, but with a little more data on the management of the network in order to direct the attack towards the desired target.

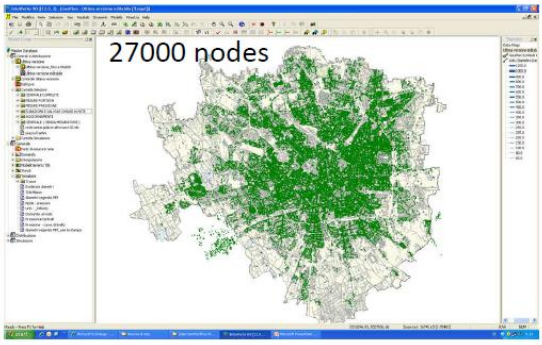
The difference between these two models of attack is similar to that between a hunting rifle and a shotgun. The first fires a great number of bullets, injuring many targets but has a relatively low mortality (although the socio-political and economic damage can be very high compared to the assets to be protected). The second instead shoots a single bullet in order to hit a 'large' target, which may have a domino effect. In both cases, however, the actor aims to demonstrate its ability to control compared to the power of any kind of government. This means that the threat always has the same profile, but what changes is the *modus operandi,* which influences the assessment of damage depending on a very large number of technical variables.

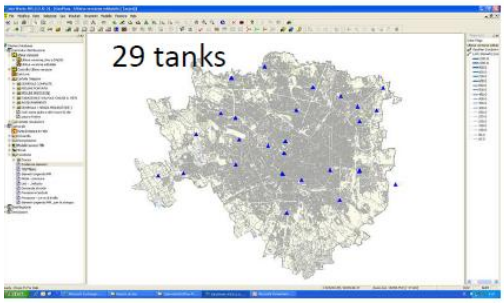
Each of these potential scenarios needs to be addressed with different instruments for the purpose of prevention and response. The node that is certainly clear from the analysis conducted in the field is that in the case of multiple attacks carried out from private residences, which in any case would result in a significant delay in response, is that greater cooperation between the public and private sectors is required. Surveillance of the territory cannot be exclusively left to the police but requires a greater degree of interagency collaboration and, above all, the participation of citizens. This is the lesson provided by the Swedish prevention model, that the Upsidedown project identified as a good practice to accompany the scenario analyses, although the Swedish model remains among the traditional methodologies of risk analysis.

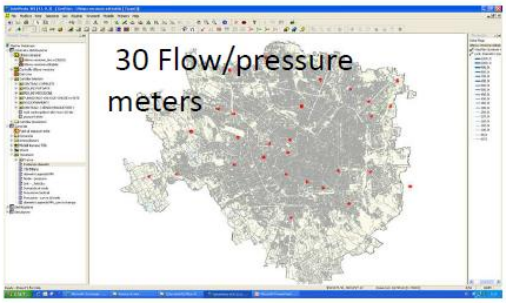
In this regard, it should finally be noted that the scenario analysis, the so-called 'What if methodology', was not limited to the analysis and testing of the easiest available scenario. Its additional contributions, worthy of being further discussed, include the development of a simulation information system, created by Metropolitane Milanesi SpA, which allows for the prediction of multiple scenarios on the basis of the technical characteristics of the water systems and the availability of existing data in the possession of the utilities or stakeholders of the governing authority.

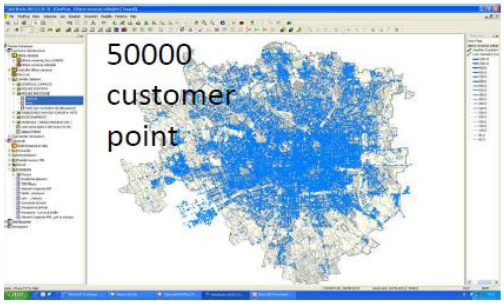
In our project we have developed a complete mathematical model, representing the whole water network of Milan. The network model, implemented using INFOWORKS WS, is composed by

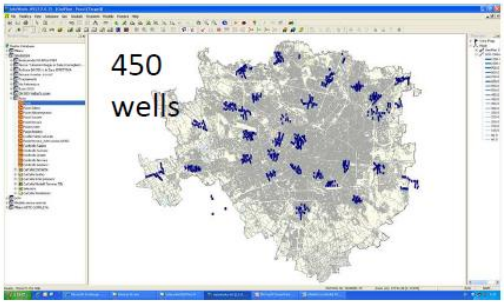












The Dynamic Water Quality model tracks the fate of a dissolved substance flowing through the network over time. It uses the flows from the hydraulic simulation to solve a conservation of mass equation for the substance within each link connecting nodes, considering mixing of fluid with different concentration.

1-Advective transport within a pipe is represented with the following equation:

$$\frac{\partial C_i}{\partial t} = -u_i \frac{\partial C_i}{\partial x} + r(C_i)$$

where Ci = concentration (mass/volume) in pipe i as a function of distance x and time t, ui=flow velocity (length/time) in pipe i, and r = rate of reaction (mass/volume/time) as a function of concentration. [Epanet]

2- Mixing at Pipe Junctions. The concentration of a substance in water leaving the junction is simply the flow-weighted sum of the concentrations from the inflowing pipes. For a specific node k one can write:

$$C_{i|x=0} = \frac{\sum_{j \in I_k} Q_j C_{j|x=L_j} + Q_{k,ext} C_{k,ext}}{\sum_{j \in I_k} Q_j + Q_{k,ext}}$$

where i = link with flow leaving node k, Ik = set of links with flow into k, Lj = length of link j, Qj = flow (volume/time) in link j, k,ext= external source flow entering the network at node k, and Ck,ext = concentration of the external flow entering at node k.

The notation Ci|x=0 represents the concentration at the start of link i, while Ci|x=L is the concentration at the end of the link.

The graphical user interface, briefly presented herein, allows even inexperienced operators to physically visualize the evolution of the potential damage based on variable parameters. This good practice, together with the IT tool that emerged from the project, deserves to be further explored so as to refine the forecasting instruments and response methods based on scenario analyses.

But most importantly, the scenario analysis has opened up a window, clearly demonstrating that the EU must urgently review the classification of critical infrastructure, incorporating those pertaining to water systems within the CIPS provisions.

ANNEX: THE BIGGEST ATTACKS ON WATER NETWORKS

EUROPE:

Date	Parties Involved	Violent Conflict or In the Context of Violence?	Description	Sources
1973	Germany	No: Threat	A German biologist threatens to contaminate water supplies with bacilli of anthrax and botulinum toxin unless he is paid $8.5 million.	Jenkins and Rubin 1978; Kupperman and Trent 1979
1994	Moldova, Russia	No: Threat	Reported threat by Moldavian General Nikolay Matveyev to contaminate the water supply of the Russian 14th Army in Tiraspol, Moldova, with mercury.	Purver 1995
1998–1999	Kosovo	Yes	Contamination of water supplies/wells by Serbs disposing of bodies of Kosovar Albanians in local wells. Other reports of Yugoslav federal forces poisoning wells with carcasses and hazardous materials.	CNN 1999; Hickman 1999
2000	France, Belgium, Netherlands	Yes	In July, workers at the Cellatex chemical plant in northern France dump 5,000 liters of sulfuric acid into a tributary of the Meuse River after they were denied workers' benefits. A French analyst points out that this is the first time "the environment and public health were made hostage in order to exert pressure, an unheard-of situation until now."	Christian Science Monitor 2000
2001	Macedonia	Yes	Water flow to Kumanovo (population 100,000) cut off for 12 days in conflict between ethnic Albanians and Macedonian forces. Valves of Glaznja and Lipkovo Lakes damaged.	AFP 2001; Macedonia Information Agency 2001
2002	Rome, Italy	No: Threat	Italian police arrest four Moroccans allegedly planning to contaminate the water supply system in Rome with a cyanide-based chemical, targeting buildings that included the United States embassy. Ties to Al-Queda were suggested.	BBC 2002
2005	Ukraine	Yes	On April 13th the Kiev Hydropower Station on the Dnieper River received a threat that 40 rail cars filled with explosives had been placed on a portion of levees holding back the reservoir.	Levitsky 2005

MIDDLE EAST:

Date	Parties Involved	Violent Conflict or In the Context of Violence?	Description	Sources
1965	Israel, Palestinians	Yes	First attack ever by the Palestinian National Liberation Movement Al-Fatah is on the diversion pumps for the Israeli National Water Carrier. Attack fails.	Naff and Matson 1984; Dolatyar 1995
1983	Lebanon	Yes	An explosives-laden truck disguised as a water delivery vehicle destroys a barracks in a US military compound, killing more than 300 people. The attack is blamed on Hezbollah with the support of the Iranian government.	BBC 2007
1983	Israel	No	The Israeli government reports that it had uncovered a plot by Israeli Arabs to poison the water in Galilee with "an unidentified powder."	Douglass and Livingstone 1987
1992	Turkey	Yes	Lethal concentrations of potassium cyanide are reported discovered in the water tanks of a Turkish Air Force compound in Istanbul. The Kurdish Workers' Party (PKK) claimed credit.	Chelyshev 1992

1993	Iran	No	A report suggests that proposals were made at a meeting of fundamentalist groups in Tehran, under the auspices of the Iranian Foreign Ministry, to poison water supplies of major cities in the West "as a possible response to Western offensives against Islamic organizations and states."	Haeri 1993
2001	Israel, Palestine	Yes	Palestinians destroy water supply pipelines to the West Bank settlement of Yitzhar and to Kibbutz Kisufim. The Agbat Jabar refugee camp near Jericho disconnects from its water supply after Palestinians loot and damage local water pumps. Palestinians accuse Israel of destroying a water cistern, blocking water tanker deliveries, and attacking materials for a wastewater treatment project.	Israel Line 2001a; Israel Line 2001b; ENS 2001a
2003	Jordan	No: Threat	Jordanian authorities arrested Iraqi agents in connection with a botched plot to poison the water supply that serves American troops in the eastern Jordanian desert near the border with Iraq. The scheme involved poisoning a water tank that supplies American soldiers at a military base in Khao, which lies in an arid region of the eastern frontier near the industrial town of Zarqa.	MJS 2003
2003	Iraq	Yes	Insurgents bomb a main water pipeline in Baghdad. City engineers say this is the first strike against Baghdad's water system during the Iraq War, which began in March 2003. The bombing occurred around seven in the morning, when a blue Volkswagen Passat stopped on an overpass near the Nidaa mosque and an explosive was fired at the six-foot-wide water main in the northern part of Baghdad, said Hayder Muhammad, the chief engineer for the city's water treatment plants.	Tierney and Worth 2003
2004	Gaza Strip	Yes	The United States halts two water development projects as punishment to the Palestinian Authority for their failure to find those responsible for a deadly attack on a US diplomatic convoy in October 2003.	AP 2004
2006	Israel, Lebanon	Yes	Hezbollah rockets damage a wastewater plant in Israel. Israeli counter-attacks damage water systems throughout southern Lebanon, including tanks, pipes, pumping stations, and facilities along the Litani River.	Science 2006; Amnesty International 2006; Murphy 2006
2007	Afghanistan	Yes	The Kajaki Dam has been the scene of major fighting between Taliban and NATO forces, mainly British and Dutch. The Taliban is attempting to make it impossible to work on reconstruction of the dam and power lines to boost output.	Friel 2007
2010	Afghanistan	Yes	A remote-controlled bomb hidden in a water truck kills three people, including two children, in the eastern Afghan province of Khost, which borders Pakistan.	AP 2009
2012	Afghanistan	Yes	Up to 150 schoolgirls are reported sickened by poison in a school water supply in an intentional attack thought to be carried out by religious conservatives opposed to the education of women.	Hamid 2012
2012	Afghanistan	Yes	Seven children are killed by a bomb thought to be aimed at Afghan police and planted at a fresh water spring in Ghor Province.	Shah 2012
2012	Afghanistan	Yes	Islamist militants execute militia members defending the Machalgho Dam in eastern Afghanistan. The dam is being developed for irrigation and local power supply. This dispute is one of several surrounding the international waters of Afghanistan, Iran, and Pakistan, which share several rivers,.	Mashal 2012

AFRICA

Date	Parties Involved	Violent Conflict or In the Context of Violence?	Description	Sources
1978–1984	Sudan	Yes	Demonstrations in Juba, Sudan in 1978 opposing the construction of the Jonglei Canal lead to the deaths of two students. Construction of the Jonglei Canal in the Sudan is	Suliman 1998; Keluel-Jang 1997

			suspended in 1984 following a series of attacks on the construction site.	
1980s	Mozambique, Rhodesia/Zimbabwe, South Africa	Yes	Regular destruction of power lines from Cahora Bassa Dam during fight for independence in the region. Dam targeted by RENAMO (the Mozambican National Resistance).	Chenje 2001
1998	Democratic Republic of Congo	Yes	Attacks on Inga Dam during efforts to topple President Kabila. Disruption of electricity supplies from Inga Dam and water supplies to Kinshasa.	Chenje 2001; Human Rights Watch 1998
1999	Lusaka, Zambia	Yes	Bomb blast destroyed the main water pipeline, cutting off water for the city of Lusaka, population 3 million.	FTGWR 1999
1999	South Africa	Yes	A home-made bomb is discovered at a water reservoir at Wallmansthal near Pretoria. It is thought to have been meant to sabotage water supplies to farmers.	Pretoria Dispatch 1999
1999	Angola	Yes	One hundred bodies are found in four drinking water wells in central Angola.	International Herald Tribune 1999
2003–2007	Sudan, Darfur	Yes	The ongoing civil war in the Sudan has included violence against water resources. In 2003, villagers from around Tina said that bombings had destroyed water wells. In Khasan Basao they alleged that water wells were poisoned. In 2004, wells in Darfur were intentionally contaminated as part of a strategy of harassment against displaced populations.	Amnesty International 2004; Reuters Foundation 2004

ASIA:

Date	Parties Involved	Violent Conflict or In the Context of Violence?	Description	Sources
1998	Tajikistan	No: Threat	Tajik guerrilla commander Makhmud Khudoberdyev threatens to blow up a dam on the Kairakkhum channel if his political demands are not met.	WRR 1998
1999	China	Yes	Around the Chinese New Year, farmers from Hebei and Henan Provinces fought over limited water resources. Heavy weapons, including mortars and bombs, were used and nearly 100 villagers were injured. Houses and facilities were damaged and the total loss reached one million $US.	China Water Resources Daily 2002
1999	East Timor	Yes	Militia opposing East Timor independence kills pro-independence supporters and throws bodies in water well.	BBC 1999
2001	Pakistan	Yes	Civil unrest over severe water shortages caused by the long-term drought. Protests began in March and April and continued into summer. Riots, four bombs in Karachi (June 13), one death, 12 injuries, 30 arrests. Ethnic conflicts as some groups “accuse the government of favoring the populous Punjab province [over Sindh province] in water distribution.”	Nadeem 2001; Soloman 2001
2001	Philippines	No	The militant Islamist separatist group Abu Sayyaf threatens to poison the water supply in Isablela, a mainly Christian town on Basilan island in the country’s south. In October, residents in six nearby villages suspected contamination due to water that smelled like gasoline. Local officials responded by closing pipelines and bringing in drinking water by truck. In the months following the 9/11 attacks on New York, numerous false alarms of terrorist activity are reported around the world.	World Environment News 2001; Fenton et al. 2001
2002	Nepal	Yes	The Khumbuwan Liberation Front (KLF) blows up a 250 kilowatt hydroelectric powerhouse in Nepal's Bhojpur District, cutting off power to Bhojpur and surrounding areas. The damages take 6 months to repair and cost 10 million Rs (US $120,000). During 2002, Maoist rebels destroyed more than seven micro-hydro projects, a water-supply intake, and supply pipelines to Khalanga in western Nepal.	Kathmandu Post 2002; FTGWR 2002

2004	Pakistan	Yes	In military action aimed at Islamic terrorists, including Al Qaeda and the Islamic Movement of Uzbekistan, homes, schools, and water wells were damaged and destroyed.	Reuters 2004a
2004	India, Kashmir	Yes	Twelve Indian security forces were killed by an IED planted in an underground water pipe during "counter-insurgency operation in Khanabal area in Anantnag district."	TNN 2004
2006	Sri Lanka	Yes	Tamil Tiger rebels cut the water supply to government-held villages in northeastern Sri Lanka. Sri Lankan government forces then launched attacks on the reservoir, declaring the Tamil actions to be terrorism. Conflict around the water blockade had claimed over 425 lives as of August.	BBC 2006b; BBC 2006c; Gutierrez 2006
2008	Pakistan	Yes	In October, the Taliban threatened to blow up Warsak Dam, the main water supply for Peshawar, during a government offensive in the region.	Perlez and Shah 2008

SOUTH AMERICA:

Date	Parties Involved	Violent Conflict or In the Context of Violence?	Description	Sources
2002	Colombia	Yes	Colombian rebels in January damaged a gate valve in the dam that supplies most of Bogota's drinking water. Revolutionary Armed Forces of Colombia (FARC), detonated an explosive device planted on a German-made gate valve located inside a tunnel in the Chingaza Dam.	Waterweek 2002
2003	Colombia	Yes	A bomb blast at the Cali Drinking Water Treatment Plant killed 3 workers May 8th. The workers were members of a trade union involved in intense negotiations over privatization of the water system.	PSI 2003

NORTH AMERICA:

Date	Parties Involved	Violent Conflict or In the Context of Violence?	Description	Sources
1748	United States	Yes	Ferry house on Brooklyn shore of East River burns down. New Yorkers accuse Brooklynites of having set the fire as revenge for unfair East River water rights.	MCNY undated
1841	Canada	Yes	A reservoir in Ops Township, Upper Canada (now Ontario) is destroyed by neighbors who consider it a hazard to health.	Forkey 1998
1844	United States	Yes	A reservoir in Mercer County, Ohio is destroyed by a mob that considered it a health hazard.	Scheiber 1969
1850s	United States	Yes	Attack on a New Hampshire dam that impounded water for factories downstream by local residents unhappy over its effect on water levels.	Steinberg 1990
1853–1861	United States	Yes	Repeated destruction of the banks and reservoirs of the Wabash and Erie Canal in southern Indiana by mobs regarding it as a health hazard.	Fatout 1972; Fickle 1983
1887	United States	Yes	Dynamiting of a canal reservoir in Paulding County, Ohio by a mob regarding it as a health hazard. State Militia called out to restore order.	Walters 1948
1890	Canada	Yes	Partly successful attempt to destroy a lock on the Welland Canal in Ontario, Canada either by Fenians protesting English Policy in Ireland or by agents of Buffalo, NY grain handlers unhappy at the diversion of trade through the canal.	Styran and Taylor 2001

1907–1913	Owens Valley, Los Angeles, California	Yes	The Los Angeles Valley aqueduct/pipeline suffers repeated bombings in an effort to prevent diversions of water from the Owens Valley to Los Angeles.	Reisner 1993
1970	United States	No: Threat	The Weathermen, a group opposed to American imperialism and the Vietnam war, allegedly attempted to obtain biological agents to contaminate the water supply systems of US urban centers.	Kupperman and Trent 1979; Eitzen and Takafuji 1997; Purver 1995
1972	United States	No: Threat	Two members of the right-wing "Order of the Rising Sun" are arrested in Chicago with 30–40 kg of typhoid cultures with which they allegedly planned to poison the water supply in Chicago, St. Louis, and other cities. Experts say the plan is unlikely to cause health problems due to water chlorination.	Eitzen and Takafuji 1997
1972	United States	No: Threat	Reported threat to contaminate water supply of New York City with nerve gas.	Purver 1995
1977	United States	Yes	Contamination of a North Carolina reservoir with unknown materials. According to Clark: "Safety caps and valves were removed, and poison chemicals were sent into the reservoir....Water had to be brought in."	Clark 1980; Purver 1995
1982	United States	No: Threat	Los Angeles police and the FBI arrest a man who was preparing to poison the city's water supply with a biological agent.	Livingston 1982; Eitzen and Takafuji 1997
1984	United States	Yes	Members of the Rajneeshee religious cult contaminate a city water supply tank in The Dalles, Oregon, using Salmonella. A community outbreak of over 750 cases occurred in a county that normally reports fewer than five cases per year.	Clark and Deininger 2000
1985	United States	No	Law enforcement authorities discover that a small survivalist group in the Ozark Mountains of Arkansas known as The Covenant, the Sword, and the Arm of the Lord (CSA) has acquired a drum containing 30 gallons of potassium cyanide, with the apparent intent to poison water supplies in New York, Chicago, and Washington, D.C. CSA members believed that such attacks would make the Messiah return more quickly by punishing unrepentant sinners. The objective appeared to be mass murder in the name of a divine mission rather than to change government policy. The amount of poison possessed by the group is believed to have been insufficient to contaminate the water supply of even one city.	Tucker 2000; NTI 2005
1991	Canada	No: Threat	A threat is made via an anonymous letter to contaminate the water supply of the city of Kelowna, British Columbia, with "biological contaminates." The motive is apparently "associated with the Gulf War." The security of the water supply is increased in response and no group is identified as the perpetrator.	Purver 1995
1998/1994	United States	No	The Washington Post reports that a 12-year old computer hacker broke into the SCADA computer system that runs Arizona's Roosevelt Dam, giving him complete control of the dam's massive floodgates. The cities of Mesa, Tempe, and Phoenix, Arizona are downstream of this dam. This report turns out to be incorrect. A hacker did break into the computers of an Arizona water facility, the Salt River Project in the Phoenix area. But he was 27, not 12, and the incident occurred in 1994, not 1998. And while clearly trespassing in critical areas, the hacker never could have had control of any dams, leading investigators to conclude that no lives or property were ever threatened.	Gellman 2002; Lemos 2002
2000	United States	No	A drill simulating a terrorist attack on the Nacimiento Dam in Monterey County, California got out of hand when two radio stations reported it as a real attack.	Gaura 2000
2002	United States	No: Threat	Papers seized during the arrest of a Lebanese Imam at a mosque in Seattle include "instructions on poisoning water sources" from a London-based al Qaeda recruiter. The FBI issued a bulletin to computer security experts around the country indicating that al-Qaeda terrorists may have	McDonnell and Meyer 2002; MSNBC 2002

			been studying American dams and water-supply systems in preparation for new attacks. “U.S. law enforcement and intelligence agencies have received indications that al-Qaeda members have sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA-related Web sites,” reads the bulletin, according to SecurityFocus. “They specifically sought information on water supply and wastewater management practices in the U.S. and abroad.”	
2002	United States	No: Threat	Earth Liberation Front threatens the water supply for the town of Winter Park. Previously, this group claimed responsibility for the destruction of a ski lodge in Vail, Colorado that threatened lynx habitat.	Crecente 2002; AP 2002
2003	United States	No: Threat	Al-Qaida threatens US water systems via call to Saudi Arabian magazine. Al-Qaida does not “rule out…the poisoning of drinking water in American and Western cities.”	AP 2003a; Waterman 2003; NewsMax 2003; US Water News 2003
2003	United States	Yes	Four incendiary devices were found in the pumping station of a Michigan water-bottling plant. The Earth Liberation Front (ELF) claimed responsibility, accusing Ice Mountain Water Company of “stealing” water for profit. Ice Mountain is a subsidiary of Nestle Waters.	AP 2003b
2007	Canada	No	A Toronto man previously accused of attempted murder and illegal possession of explosives is charged with eight more counts of attempted murder after allegedly tampering with bottled water, which he injected with an unspecified liquid.	Toronto Star 2007