Journal of Earth Sciences and Geotechnical Engineering, Vol.11, No.1, 2021, 65-107
ISSN: 1792-9040 (print version), 1792-9660 (online)
https://doi.org/10.47260/jesge/1113
Scientific Press International Limited

Dam Safety: Hazards Created by Human Failings and Actions

Nasrat Adamo[1], Nadhir Al-Ansari[2], Varoujan Sissakian[3], Jan Laue[4] and Sven Knutsson[5]

Abstract

Dam Safety and dam incidents are treated here looked at from the "Human Factors" perspective. An attempt is made to explore these factors as an important drive in impairing dams' safety and increases their risks. Distinction is drawn between the "Normal Human Caused Incidents" and the "Extraordinary Human Caused Incidents" together with the description of their root origins and subsequent consequences. The first type includes unintentional mistakes, errors and flaws committed by the operators of dams inadvertently, in addition to negligence, lack of experience or overconfidence. Such failings can happen in manual operation of dams, or through the use of their Supervision, Control and Data Acquisition (SCADA) systems as in industrial control system (ICS). They can occur also due to flaws in software or even in the application of information and communication technology (ICT) in remote control operations. As for the second group; the extraordinary human factors, they are defined here as those committed by man with the full understanding of their possible damage. They are done purposely for destabilizing dams after thoughtful and carefully meditated decision making process and they are manifested in acts of war, sabotage and terrorists actions. In this modern age, these acts are characteristics of hackers' attacks on dam(s) operating systems. This is done through the use of cyberspace by the widespread interconnected digital technology with the accompanying advances in the communication technologies. As such, these technologies have made remote control of such systems possible. Not limited to this, dams remain now, as they were

[1] Consultant Dam Engineer, Sweden.
[2] Lulea University of Technology, Lulea 971 87, Sweden.
[3] Lecturer, University of Kurdistan Hewler and Private Consultant Geologist, Erbil.
[4] Lulea University of Technology, Lulea 971 87, Sweden.
[5] Lulea University of Technology, Lulea 971 87, Sweden.

Article Info: *Received:* September 7, 2020. *Revised:* September 17, 2020.
Published online: September 28, 2020.

always in the past, the obvious targets in wars and conflicts to inflict losses on the enemy and to use them as weapons, and for terrorism actions for challenging governments. Examples of the aforementioned threats are described with examples given from real cases to elucidate the dangers involved. Lessons to be learned from these incidents are derived and recommendations are presented to be followed to avoid risky situations.

Keywords: Normal human caused incidents, extraordinary human caused incidents, SCADA Systems, ICS System, software, ICT Technology, cyberspace, digital technology, remote control, hackers, terrorism.

1. Introduction

While safety hazards of dams can be created by improper planning, faulty design, or result from improper selection of site and dam materials and construction procedures, such hazards may also be intensified by human actions or inactions, and they may be intentional or unintentional throughout the decision making processes and during the operation of the dam. Description of such hazards supported by case histories can help illustrating the nature of the problems involved and help to draw lessons from them. They may also guide in taking precautionary or protection measures. But it is not enough; however, at just discovering the single prime cause of such events if the full lesson is not learned; any study cannot serve its purpose without tracing the chain of actions and interactions leading to the failure or accident. This implies that dams should be treated as systems containing many interacting components and subsystems and that the root of the problem may be hidden in a single action within the chain of events leading to the undesirable end. Or, more often it can mean that one component of the dam system is more critical to dams safety than others. One distinction must be made right at the start between two major types of accidents. The first category concerns what is called “Normal” accidents, or system accidents, which result from human actions; the second type are those which are imposed on dams from outside but also through human actions and shall be called here “Extraordinary” incidents. Normal accidents are inevitable in extremely complex systems, and given the characteristic of the system involved, multiple failure drives interacting with each other can occur, despite efforts to avoid them. One example is operators’ errors, which are quite common problems, while many other failure drives relate to organization; rather than technology or individuals’ actions. It is also common that big accidents almost always have small beginnings. Such events appear trivial to begin with before unpredictably cascading through the system to create a large event with severe consequences. So “Normal” accidents are spontaneous and are related to the nature of the dam and its operation as a system [1].

The “Extraordinary” incidents, on the other hand, are those caused by man for purposely destabilizing dams after thoughtful and carefully meditated decision making process which is manifested in sabotage and acts of war. Brief reviews of

both types are given here with some illustrations.

2. Normal Accidents and the Human Factors

No system has ever built itself, and since few systems operate by themselves, and since no systems maintain themselves, the search for a human in the path of failure is bound to succeed. If not found directly at the sharp end, as a "human error" or unsafe act, it can usually be found a few steps back [2].

This was the conclusion reached by Professor Richard J. Holden from the University of Wisconsin- Madison covering professional safety management, which applies to man-made systems; and dams are no exception.

Dams as systems typically include both human and physical elements, and are sometimes referred to as "sociotechnical" systems. To prevent future dam accidents, it is essential that dam safety professionals understand both the physical factors and human factors, and how they contribute to failures or safety hazards.

Physical factors stem from forces and situations imposed on dams by natural events of floods and earthquakes. Foundations and dams' materials create the spectrum of other potential unsafe conditions. But, while these factors can be calculated and quantified to a high degree of refinement, mistakes or bad judgments can still creep into this defeating the purpose of safety considerations. Human factors contributing to the potential for failure can also result from pressures imposed on designers by the requirements of more water and power generation, or by constructors and owners trying to meet time schedules or even by maintenance constraints due to budgeting problems.

In the operation phase, human misjudgment associated with faulty memory, ambiguity of instructions and incompleteness of information play negative roles, while experimenting with untried shortcuts may bring undesirable outcomes. In critical situations, while operating personnel are facing dangerous occurrences psychological conditions; fatigue and emotions can lead to grave mistakes and undesirable ends. Lack of knowledge, lack of expertise and even negligence is more of the other factor that have contributed to some dams' incidents and failures.

Human errors and the underlying primary drivers of failure noted above often lead to inadequate risk management. Inadequacies in risk management may be classified into three types:

- *Ignorance* which involves being insufficiently aware of risks. This may be due to aspects of human fallibility and limitations such as lack of information, inaccurate information, lack of knowledge and expertise, and unreliable intuition. Complexity can also contribute to ignorance.
- *Complacency* which involves being sufficiently aware of risks but being overly risk tolerant. This may be due to aspects of human fallibility and limitations such as fatigue, emotions, indifference, and optimism bias that "it won't happen to me". Pressure from non-safety goals can also contribute to complacency.
- *Overconfidence* involves being sufficiently aware of risks, but overestimating the ability to deal with them. This may be due to aspects of human fallibility

and limitations such as inherent overconfidence bias, which results in overestimating knowledge, capabilities, and performance [3].

In modern procedures applied to various systems, including dams, pitfalls in control software may appear in untried situations; similarly, an unexpected failure of one element of the software can cause dangerous conditions. In such cases, alarm signals might be wrongly interpreted, or operation commands are not correctly received. The more complex the system is, the more are the possibilities of wrong interactions. Such interactions can result in large effects from small causes, including "tipping points" when thresholds are reached, and they make complex systems difficult to model, predict, and control. Complexity, generally exacerbates the effects of human fallibility and limitations. An example of this from the aviation industry is the flaws were embedded in the control software leading to the two Boeing 737 max 8 catastrophes in 2018 and 2019. Software known MCAS which was supposed to ensure the plane flew smoothly was expanded in 2017, but the new version installed in the plane was risky as it relied on single sensor that could push down the nose of the plane by a much larger amount. Regulators had never independently assessed the risks of this, which led eventually to these catastrophes of 346 peoples being killed in the two plane crashes.

As far as human factors are concerned, the following six aspects are key observations regarding past failures of dams and other systems:

- Failures are typically preceded by interactions of physical and human factors, which begin years or decades prior to the failure.
- The interactions among physical and human factors are often not simple and not linear. Instead, they may be complex and involve nonlinear relationships, feedback loops, causes having multiple effects, effects having multiple causes, and a lack of distinct "root causes" or dominant contributing factors.
- Interactions among physical and human factors usually generate "warning signs" which are not recognized, or not sufficiently acted upon, prior to the failure.
- Physical processes deterministically follow physical laws, with no possibility of physical "mistakes." Therefore, failures, in the sense of human intentions not being fulfilled, are fundamentally due to human factors, as a result of human efforts individually and collectively "falling short" in various ways. A story of *why* a failure happened; therefore, cannot be complete without reference to contributing human factors.
- A natural tendency is for systems to move towards disorder and failure, in line with the concept of increasing "entropy" in physics. Therefore, systems such as dams are typically not inherently "safe," and continuous human effort is needed to maintain order and prevent failure.
- Systems such as dams, including the people involved in designing, building, operating, and managing them, tend to conservatively have numerous "barriers" which must be overcome for failures to occur. This generally makes failures unlikely and results in low overall failure rates. However, when dealing with a

large number of systems, such as the approximately 90,000 dams in the United States, it can be expected that "unlikely" failures will sometimes occur, due to physical and human factors "lining up" in an adverse way that overcomes all barriers [4].

3. Dams incidents Caused by Human Factors During Operation

3.1 General

Dams have been operated traditionally by trained personnel some of whom are residing on site, manning all operations from a control center located within the site. Some of the operating team are always on duty, and this will depend on the size and importance of the dam. In case of a sudden event, such as an unexpected strong storm or an earthquake, then immediate safety actions can be taken such as opening spillway or outlet gates to relieve the pressure on the dam or to call for help from outside to support the effort and to declare emergency situation if needed and even sound the alarm for starting an evacuation effort for the threatened communities downstream. Moreover, any malfunctioned control equipment during this event would be put right in time, and bad consequences can be averted. All this sound as good and well thought of practice, but many dam failures have resulted either from bad management during emergencies, or through negligence and carelessness or from overconfidence and short sight caused by lack of knowledge and false confidence that nothing adverse will happen.

The same thing occurs from having the notion that whatever happens it can be mastered and solved in time. With the progress being made in technology, and in no doubt under economic pressure, new technologies have been introduced in the control and operation of dams. It is assumed that the new technologies can bring the same degree of safety, if not better, as manual operation. Advances made in modelling and simulation techniques and software advances, in addition to high tech communication systems, have given a higher confidence in this field. Ironically, these same technologies have also contributed to some incident and failures in the same way as what had happened in the Boeing 737 Max 8 cited before. In operating a network of dams, whether in flood control or power generation, the control is left to a single or very few persons tending to this by remote control operation systems; while sitting in remote control centers away from the dam site(s). Decisions are made depending on a Supervision, Control and Data Acquisition (SCADA) systems without directly seeing the structure(s). Any fault creeping into these systems, or any wrong interpretation of the data streaming or recorded by the monitors, can lead to an incident or failure which may go undetected for an additional time leaving no chance to take any quick remedy. Similarly, spillway gates are now seldom operated by a dam tender going to the dam crest and pushing a switch that directly allows operation of the gate motor. Now, a remote operator may click a virtual button on a computer screen. In the first case, the dam tender gets immediate visual feedback that the proper gate is indeed moving or not. In the second case, the remote operator

gets a signal that the gate is moving from some form of position sensor. If the sensor is giving erroneous data, the operator has no real knowledge if the gate is moving or how far it is moving. The loss of positive confirmation of gate position would result in a gate being raised far in excess of the operator's intentions and larger than intended release of water causing damage in the downstream reach. In the following, some examples of recorded cases are given.

3.2 The Euclides da Cunha Dam case: An Example of Over Confidence

Euclides da Cunha Dam in Brazil was built in 1958 and failed on January 19, 1977.This dam was 40 m high and 300 m long, and stored 25 Km^3 of water. For a catchment area of 4,300 km^2, the gated spillway capacity was 3,000 m^3/sec. The inflow was calculated to be 2,000 m^3 /sec during the event of a storm, but the two radial gates were kept closed due to human error when the operating crew stayed for lunch and when returned, as a cause of heavy rainfall, the access road had become impassable. The embankment withstood seven hours of overtopping up to one meter until it breached, and the breach width was limited to 100 m. The maximum discharge of flood from failure, which was in the range of 10,000 m^3/sec, caused the failure of the dam. The flood destroyed also the 41m high Annan does de Salles Oliveira earthfill dam at the downstream. However, there were no fatalities. The dam was rebuilt with an additional (free-flow) spillway. This is a case of overconfident operators of nothing out of the ordinary can happen during their absence from the site, and if anything happen, then they can control it, both assumptions proved to be wrong. While the overconfidence of the designer, that nothing of this sort was possible, resulted in brushing aside the need of the extra safety of a free flow emergency spillway [5] and [6].

3.3 Failure of Dibis Dam; An example of Negligence and Bad Management

This dam is located on the Lesser Zab River in Iraq approximately130 km upstream from its confluence with the Tigris River. The purpose of the dam is to divert water from the Lesser Zab River into the Kirkuk Irrigation Project main canal. It was constructed between 1960 and 1965 as part of the larger Kirkuk Irrigation Project for the irrigation of 300,000 hectare of very fertile land. Dibis Dam as designed is a 23.75m high earthfill dam made of gravel-alluvial fill material and concrete diaphragm central core, combined with concrete section forming the gated spillway structure. Figure 1 shows the spillway of this dam.

Figure 1: Dibis Dam in Iraq [7].

The spillway has a capacity of 4,000 m^3/sec through the gated structure while additional discharge of 278 m^3 /sec can be passed through the head regulator of the Kirkuk Irrigation Project which is located at the upstream right side of the dam. Inflow to the dam is from the upstream Dokan Dam releases and from any flow discharge that originates from the intermediate catchment between the two dams which contribute considerable runoff during heavy rains.

On the night of 1st of March 1984, the dam failed during an intensive rain storm which coincided with large inflow from Dokan Dam. The fuse-plug that should have worked in such rare occurrences did not erode; the local authorities constructed a concrete slab for road and for passing a large diameter water supply pipe. The operator had left the site to spend the night in his home in Kirkuk with the gates partially open without leaving replacement to operate the spillway radial gates in case of emergency as the one when the flood occurred. Combination of a high flow release from Dokan Dam with remarkably high runoff from the intermediate catchment caused the overtopping and erosion of the earthfill embankment completely leaving the spillway intact. The fuse plug intended to erode to prevent failure in such a case did not work.

Unofficial sources put the number of fatalities at nine. The dam operator was charged with manslaughter and sentenced to life imprisonment, while the engineer

in charge of dam administration stationed in Kirkuk was sentenced to nine years imprisonment for lack of attention and faulty management, in addition to the Director General of the State Organization for Dams and Reservoir (SOD) in Baghdad being dismissed. The dam was rebuilt again between October 1985 and March 1987 [7].This failure is a clear case of negligence, which aggravated a situation already compromised by other failings and bad management. Leaving the site unattended by the operator without permission was only the final mistake in a series of mistakes. The dam engineer, living in Kirkuk and not on the dam site, could not have paid enough attention to dam safety issues in such a situation or in any other risky situation and even lacking the ability to provide operators replacement if needed. Failure of SOD in Baghdad, to provide enough residence facilities at the site could have contributed to this. Moreover, allowing the construction of concrete paved road and laying of large diameter water supply pipe on top of the earth embankment, with or without knowledge of the Engineers office or this organization, was the most hideous and outrageous act of ignorance, which nullified the fuse plug function that could have stopped crest erosion FAILURE as intended by the designers. The Consultant of the project should have, in any case, put special emphasis on this matter in the project (O & M) report, but he did not do. The absence of a dependable communication system between the two dams, the dam engineer office and with the main office in Baghdad is one more management gap that otherwise could have stopped this event by ordering the Dokan Dam office to reduce or even stop altogether the release from that dam.

3.4 Nimbus Dam Incident: A case of Technological Failure and Human Interaction

The Nimbus Dam was completed in 1955 and measures approximately 75 feet high and 1,090 feet in length. The dam serves as an afterbay structure for Folsom Dam to reregulate flows of the American River for flood control, and as a diversion dam to direct water into the Folsom South Canal, while at the same time serving as a forebay for the hydroelectric generation station. Nimbus Dam includes two generators capable of producing more than 15,520 kilowatts of power. As a regulating reservoir, variations in water levels on Lake Natoma occur daily, but are generally only between two and four feet. Flow control is accomplished through 18 radial gates with individual gate bays as shown in Figure 2 [8].

A case of hazardous situation generated by technological failure had developed in this dam during operation routine, but it was relieved by human intervention, and therefore, is worth mentioning.

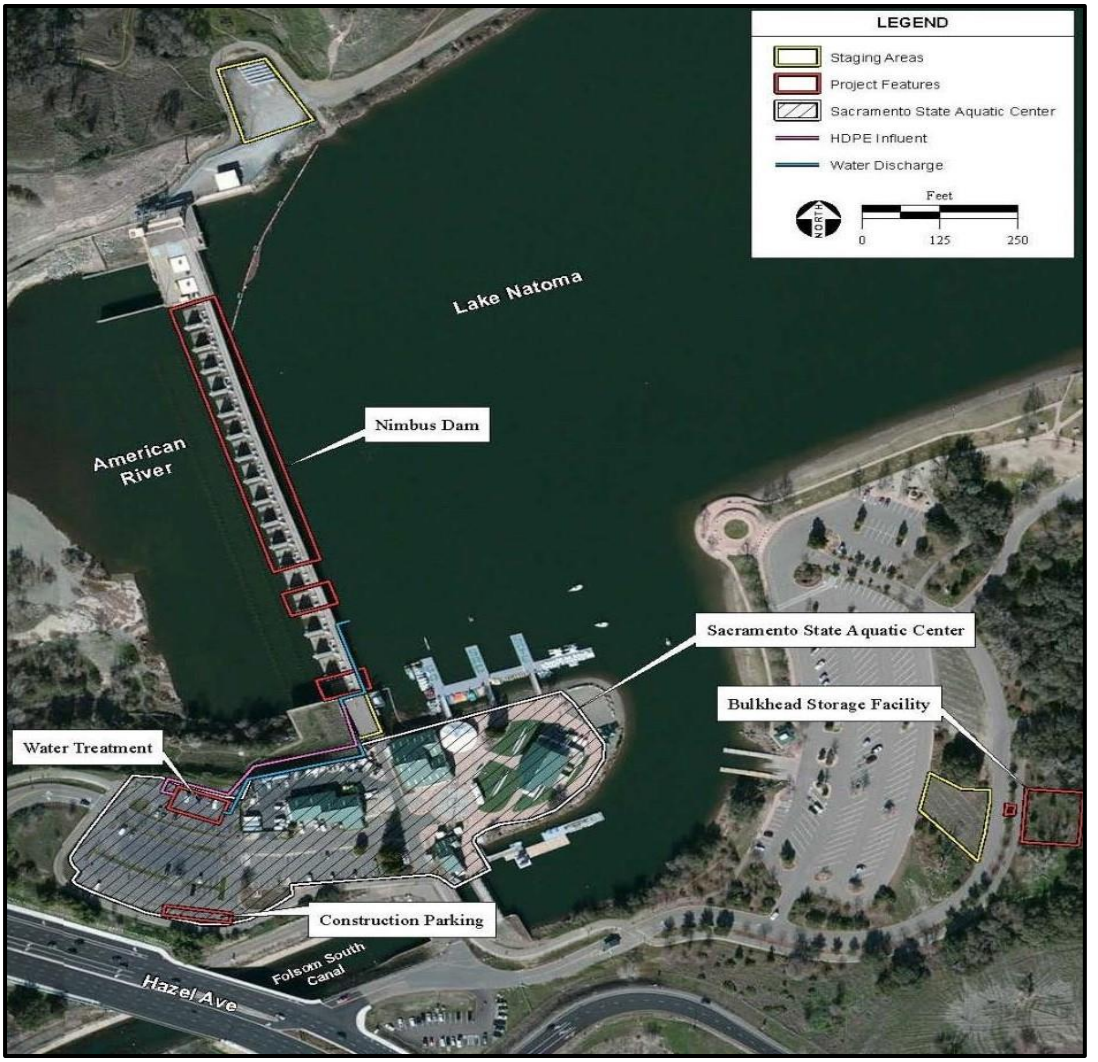

Figure 2: An aerial photograph of Nimbus Dam [8].

The exact scenario of the incident was played out at the Nimbus Dam on one Saturday of February 2006 when a loose electrical connection on one gate broke as a result of gate vibration caused by the water gush. As a consequence, this resulted in the failure and malfunctioning of the respective control sensor and caused the gate to open for 30 minutes raising the water level in the river by 5½ feet. Fortunately, this happened with only one gate, and for thirty minutes the gate stayed wide-open. It was the first serious malfunction in the gate control system, which was installed about two years before.

The problem occurred at 1 p.m. Saturday as four of the dam's 18 gates were being opened slightly to increase the flow of water downstream of the dam from 5,500 to 7,000 cubic feet per second. The malfunction caused one of the gates to fully open, increasing the flow to about 20,000 cubic feet per second.

One of the observers comments on the incident was reported as saying: “When you raise the gates, there's a sensor that is supposed to kick in and stop the gates from opening beyond a set point, when the sensor failed, one of the gates continued to open”.

According to a U.S. Geological Survey chart, a flow increase from 5,500 cfs to 20,000 cfs raises the river's average depth from 7.2 feet to 12.7 feet.

The gate remained open for about 30 minutes before an operator closed it using a manual override switch on top of the dam. The loss of positive confirmation of gate position resulted in a gate being raised far in excess of the operator’s intentions and in larger than intended release of water causing the stranding of people in the downstream reach. But human interaction at the right time had stopped a technological failure from creating a very hazardous situation [9]. This case illustrates a positive human interaction which has stopped flooding of the downstream and highlights the vulnerability of technology in systems such as dams.

3.5 The Taum Sauk pumped storage plant Failure: An Example of Complex Interactions of Human Factors, Technological Errors and Society Demands

The Taum Sauk pumped storage plant is a power station in the St. Francois mountain region of Missouri, United States about 140 kilometers south of St. Louis near Lesterville, Missouri [10].The plant was constructed from 1960–1962 and was designed to help meet daytime peak electric power demand. It began operation in 1963. The plant consists of a lower reservoir, which is sited along the East Fork of the Black River, and an upper reservoir, which is formed by a kidney-shaped rock-fill dike approximately 15.2 to 26.5 meters high, capped by 3.05 meters concrete parapet wall set on a crest that is 3.66 meters wide.

The upper reservoir held 5.67 million cubic meters when filled. A variety of design/construction flaws, an instrumentation programming error together with other human errors contributed to the failure of the upper reservoir on December 14, 2005.

Malfunctioning and improperly programmed, and placed sensors failed to indicate that the reservoir was full and did not shut down the facility's remaining pump unit water had been overflowing for 6 to 7 minutes. This overflow undermined the parapet wall and scoured the underlying embankment, leading to a complete failure within that time frame. The peak discharge from this outbreak flood was estimated to be 8,184 m^3/s, obliterating most of Johnson Shut-ins State Park, where, miraculously, only five people were injured. The flood pulse was significantly mitigated by capture within Lower Taum Sauk Reservoir, and the maximum discharge over the Lower Taum Sauk Dam was limited to just 45.3 m^3/s, precluding any significant downstream damage [11] and [12]. The photograph in Figure 3 taken below panel 71-72 of the parapet wall shows the deep plunge pool that developed and the subsequent undercutting of the wall, while Figure 4 indicates arrows representing the outflow nape once it extended beyond the wall footing and directly onto the underlying rockfill. The rate of scour and erosion increased dramatically once this occurred.

The failure of Taum Sauk was not due to a single easily identified cause that was initiated on the fateful day. The failure began the day the project was conceived, and the failure was the result of many seemingly unrelated decisions and systems that interacted in complex ways that were not anticipated [13].

Figure 3: This photograph taken below panel 71-72 shows the deep plunge pool that developed and subsequently undercutting of the parapet wall [3].

Figure 4: photo shows arrows representing the outflow nape once it extended beyond the wall footing and directly onto the underlying rockfill. The rate of scour and erosion increased dramatically once this occurred [3].

The sequence of events from overtopping of the parapet wall until wall section collapses is explained in Figure 5. The rockfill dam was washed away while the failed section of the parapet wall overturned and collapsed. The progress of erosion of the dam embankment until the development of the breach is illustrated in enlarged diagrams as shown in Figure 6. The remnants of the lip as seen at the site of failure is shown in a photograph of Figure 7.

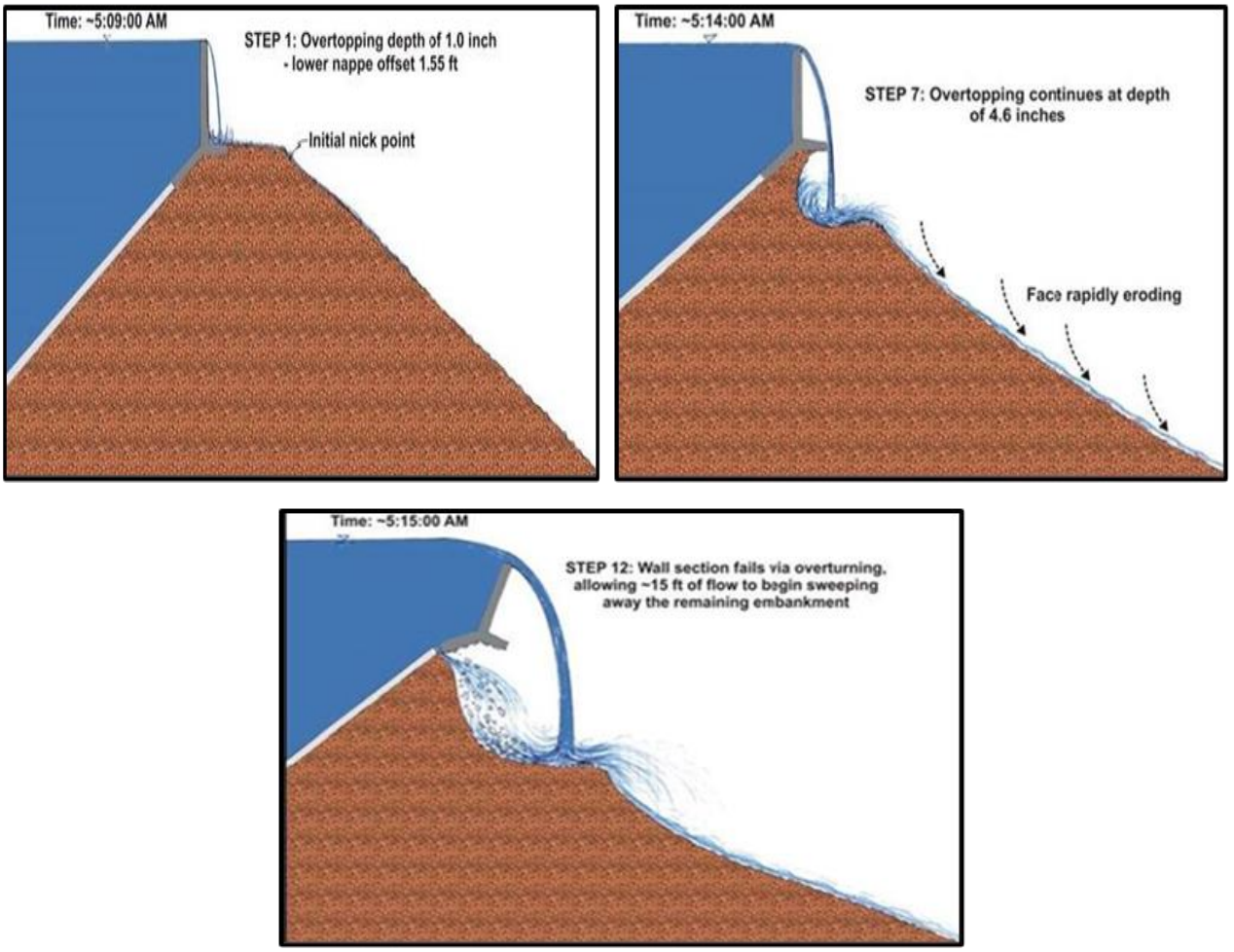

Figure 5: The sequence of event from overtopping the parapet wall until wall section collapses [3].

After failure of the dam, several investigation reports were prepared in an effort to identify the causes of the failure. The failure scenario was a case of overtopping of one section of the parapet wall on top of the reservoir dyke crest resulting in its collapse and leading to the release of water, which eroded the downstream slope of the dyke. Erosion was due to the rapid rise in phreatic surface and pore pressure in

the dyke's fill. The collapse of the parapet wall section itself had happened when overtopping of the parapet wall had locally undermined its footing leading to its sliding and overturning. The reports agreed that; the water level monitoring instrumentation was wrongly set so that their sensors gave a lower level of water than real, and with the absence of visual confirmation of water level and lack of an emergency spillway, were all primary contributing causes to the failure. The same reports also identified the weak foundation conditions of the rockfill dyke and its low shearing strength together with the operation and maintenance of the dam itself were all secondary causes. The failure of the parapet wall which initiated the failure processes was taken as a tertiary contributing cause.

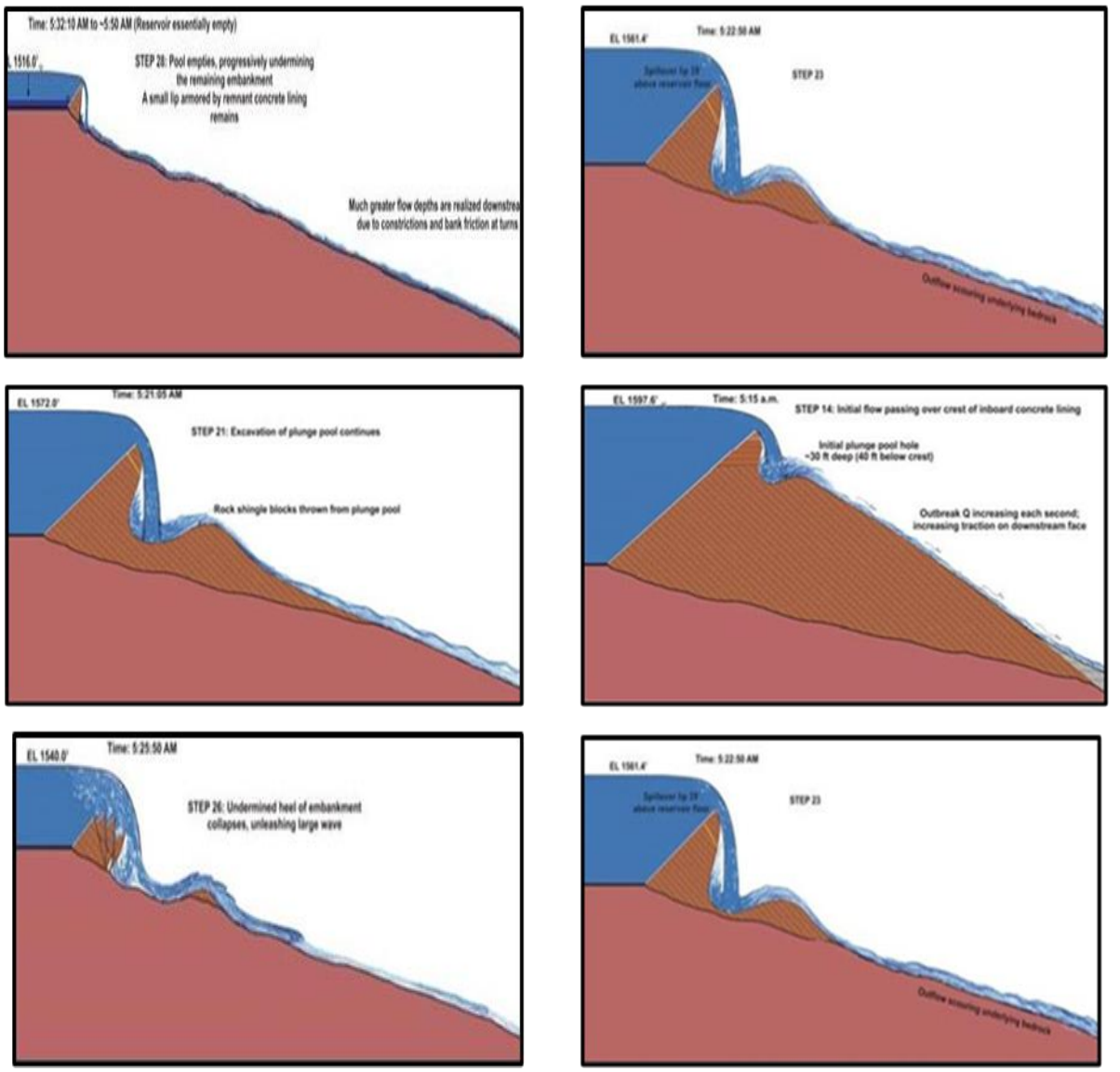

Figure 6: Progress of erosion of the dam embankment until the development of the breach [3].

Figure 7: Photograph showing remnants of the lip as seen at the site of failure [3].

Summarizing, post-breach inspections and evaluations revealed the following information timeline:

1. The project historically operated with a minimum of two feet of freeboard on the lowest section of the parapet wall. Following installation of a geomembrane liner in 2004, the owner operated the project to fill the upper reservoir within one foot of the lowest section of the parapet wall. Post breach evidence shows the reservoir may have been routinely filled to within 0.25 foot of the lowest section of the parapet wall.
2. The December 14, 2005 breach was preceded by a significant wave overtopping that occurred on September 25, 2005.
3. On September 27, 2005, the owner's personnel adjusted the reservoir control programming to account for the difference between the actual reservoir levels and the readings from the reservoir level instrumentation as such difference was visually observed.
4. On October 3-4, 2005, the owner's personnel discovered that the conduit which housed the instrumentation for monitoring reservoir levels was not properly secured to the dam. Deterioration of the instrumentation tie-down allowed the conduits to move adversely impacting the reservoir level readings instrument. The instrumentation readings showed reservoir levels that were lower than actual levels. As a safety measure, the owner's personnel adjusted the reservoir level control programming to shut down the pumps when the instruments showed the reservoir levels were two feet lower than normal settings. Figure 8 shows the deflected conduits of the cables and the foot note below it explains the sequence of events leading to this event.

5. Two new conductivity sensors were installed as a safety system for shutting down the units in case of high water levels. The sensors would send a signal to shut down the units when they became wet. The sensors were mistakenly relocated to a height that was higher than the lowest point on the parapet wall. Therefore, if the new sensors were contacted by water, the Upper Dam would already be in an "overtopping" condition.
6. Modifications made to the reservoir control programming adversely affected how the signals from the new sensors were managed and reported. The modifications required that both sensors contact water to initiate shutdown. This removed a layer of redundancy to the safety system [14] and [15].

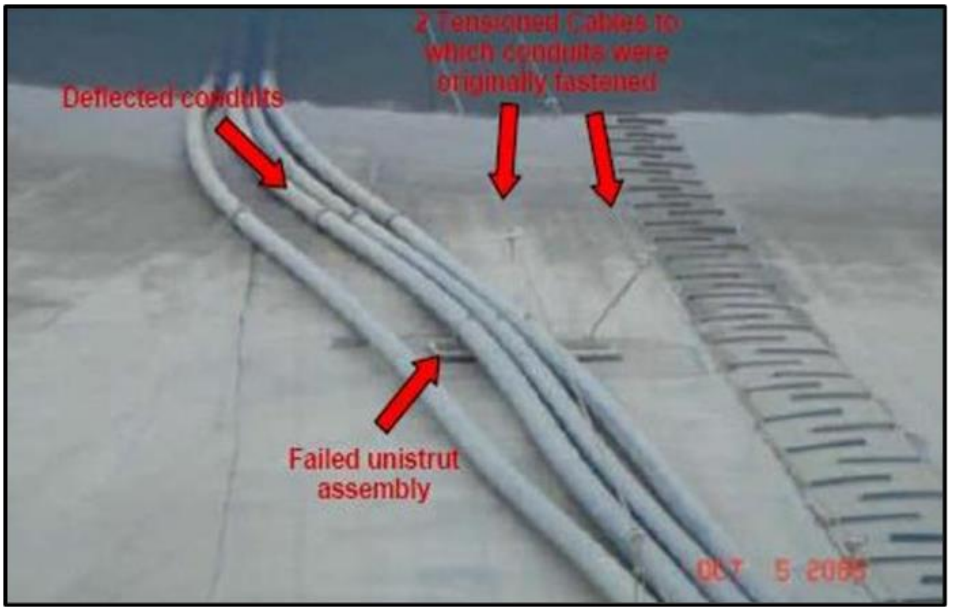

Figure 8: Deflected conduits at Taum Sauk Dam reservoir.

Note: Deflection of the instruments cables conduits was caused by the swirling action of water in filling/emptying of the reservoir. This was due to the proximity of the conduits to the inlet/outlet water shaft of the power station. This deflection was created after replacing the concrete lining by geomembrane and the failure of the tie down system to secure the conduits in its right position.

Now looking at this case as an unfortunate chain of actions, reactions and interactions, it is clear that many nodes on this chain were pushing towards the final outcome. Decisions made, and other ones not taken had sealed the fate of the project since the beginning and throughout its life. Selecting the location of the upper reservoir, design and implementation of the reservoir dyke and its parapet wall, replacing the concrete lining by geomembrane and choice of the tie down method of conduits, and the choice of the instrument cables conduits location close to the inlet/ outlet of the power station shaft are all examples of unfortunate decisions. Missed decisions which could have improved safety conditions would have been:

- If control feedback systems were provided.
- If an emergency spillway was constructed.
- If larger free board allowing for higher dyke settlement was considered.
- If a decision was made in the design stage to locate the water level measuring instruments away from the location of the inlet/outlet water shaft so would not have subjected the instrument cables conduits to the vortices and swirling of water going in and out of the shaft causing its shifting position leading and the instrument to indicate erroneous safe freeboard and therefor delaying shutting down of the pumping unit causing overtopping.

The final act which to say, the straw that broke the back of the camel, was the one dictated by society demanding more power at time of intense competition between utilities, which pushed the owners to delay repairing the water level measuring instruments until the normal outage for general maintenance.
The intense competition came as a result of deregulation of the electric market which meant that utilities were no longer guaranteed a rate of return on investment. Rather, in the emerging free market, utility profits were driven by market conditions. In December, 2005, the Taum Sauk pumped storage project provided significant financial benefits to its owner. For this reason, repairs were delayed until the planned future shutdown. In such case, safety was compromised by the competing goals of profitability and reliability as the repairs were delayed.
In final judgment, it should be noted here that the control equipment did not fail. The shutdown system behaved exactly as programmed but, unfortunately, the programing of the water level measurement was erroneously set, and this was a grave human failure. Moreover, even the erroneous readings of these equipment's were not a sufficient reason for the failure by themselves, but when compounded with other human mistakes and failings led to failure.
Construction of a new Upper Reservoir for the Taum Sauk Pump Storage Plant took place from 2007 to 2010. Today the reservoir is impounded by a roller-compacted concrete dam that is equipped with a multitude of safety features and appurtenances that adhere to current standards [16].

4. The Extraordinary Incidents and the Human Factor

4.1 General

The category of "Extraordinary Human Caused Incidents", occur not as "Normal Accidents", but result from thoughtful and carefully meditated decision making human process for the purpose of destabilizing dams or any other strategic or economic system. These have been manifested in the long history of dams in acts of war or sabotage, and in modern history by cyber-attacks which aim at disrupting the normal operation of dam or system of dams, leading to substantial deviation from the operational state as per design intents. The final objective is creating an unacceptable risky condition and damage.
History tells that using water released from dams or canals was an old used war

tactic to destroy enemy troops, or prevent their advance, or even facilitate own army advance. Cyrus the Great reputedly took Babylon in a single night in the 6th century, B.C., by diverting an old artificial lake back into the Euphrates, so that his army could come right up to the city walls at night.

Hulagu, who destroyed medieval Baghdad in 1258 A.D. used the Tigris River flood waters to trap the caliph's horsemen outside the city walls; and, the Mongols also destroyed the medieval city of Gurjang in Central Asia by breaching a nearby dam, making it an example of those who dared resist their advance.

In the 1980s, both Iran and Iraq used water as an area denial weapon to check the other's advance in southern areas of both countries. Iran tried to bomb Iraqi dams out of commission, and Iraq retaliated in the same way in the first Gulf War. USA and the Coalition air forces did exactly the same thing in the Second Gulf War to knock out hydropower stations such as that of Mosul Dam. These acts were all done while the 1977 Geneva Conventions specifically outlawed the targeting of water infrastructure in wartime.

Spectacular water warfare methods used in recent times are still vivid in the human memory. In the Second World War, the occupying Germans broke dikes in Netherland to try to halt the Allied advance. This did not delay the Allies much, but it did destroy about a quarter of the country's total farmland ahead of a very bitter winter. The Allies also blew up dikes in The Netherlands for tactical purposes, but not on a large scale. The Germans also flooded terrains in Italy in order to deny them to the Allies, leading to terrible malaria outbreaks. Adolf Hitler reserved the worst for his own Reich; however, his scorched-earth "Nero Decree" would have destroyed the German hydroelectric and flood control systems on the cusp of German defeat in 1945; if it were not for wise German officials who declined to carry out the suicidal order.

The British, being on the verge of defeat by the Germans, did not hesitate from committing the same type of atrocities when the RAF carried out the famous dam-busting action in Europe in World War II. The flooding from the breaches killed more than a thousand German civilians plus many Allied prisoners trapped in downstream camps.

In one case, the sheer loss of life of one area-denial far surpassed any chastise. Hundreds of thousands of Chinese civilians died when the Nationalist Chinese breached the Yellow River dikes in June 1938. Nationalist generals planned to "use water as a substitute for soldiers" during the battle of Wuhan, which proved to be a hasty decision. Nationalist soldiers bombed and hacked at the dikes for days until the first breach took place on June 9. There was no coordinated evacuation for the people in the water's path, nor even many early warnings. Most officials had already fled ahead of the Japanese army and very few households had radios or telephones. Neither the retreating nationalists nor the Japanese occupiers provided much relief to the survivors. And no civilian aid organizations could get into the disaster zone due to the fighting. Owing to the flooding, the Japanese army had to give up on its immediate target, the city of Zhengzhou. The floods failed to immediately halt the main Japanese offensive on Wuhan, but the city fell in October 1938.The

Nationalist government tried to blame the disaster on the Japanese even though refugees, the military, and the foreign press all knew quite well that Chinese spades and mortars were responsible [17]. The increased use in modern times of dams and water structures as targets by terrorist groups to achieve political ends has undermined the safety of those infrastructures. This has led in the meantime to increased governments worries and increased dam hazards.

In the recent technological and scientific revolution, new threats from the "Human Factors" have resulted from the interference with modern technologies by wrong manipulation, which can destabilize and hit systems used in dams.

A recent report prepared by the Office of the Inspection General of the US Bureau of Reclamation under the title "External direct impacts- Selected Hydropower Dams at increased Risk from Insider Threats" presented this by explaining that the world is witnessing an ever expanding revolution in the networked information infrastructure that blends computing, and communications and this may be considered as the greatest achievement in human history. So, during the last two decades advances in the information and communication technology (ICT) have fundamentally reshaped the management policies and control procedures of complex systems all over the globe making great savings in costs and increasing flexibility in operation, but the report adds that this has increased at the same time the threats from human factors.

In the two dams examined by the Bureau, "Direct Threats" on the Bureaus' dams were considered minimal since the operation (ICT) systems were isolated and independent from the internet and from the USBR's business systems. The report, however, warns from the "Indirect Threats" coming from accounts management and personnel security practices, which puts the control ICS and the infrastructure they manage at high risk from insiders' threats.

Typically, loop holes can develop from failure to limit the number of ICS users who have administrator access and having an extensive number of group accounts, which can allow "Hackers" creeping in together with the noncompliance with password policies and failure to remove inactive system administrator accounts.

The report also warns against not following best security practices so it recommends that personnel with elevated system privileges complete more rigorous background investigations. Deficiencies, in the words of the report, have occurred because USBR management failed to strengthen the Bureau Risk Management Practices in response to rapidly escalating threats of modern warfare and cyber-attacks. The report even went further to cite spectacular examples from recent years, including targeting electric power generators and distributors in the Ukraine by infecting control systems that operate the infrastructure. This was linked to Russia, which was accused of using sophisticated malware [18].

Recognizing the grave consequences, it was in 2016, that for the first time, the Industrial Control Systems Cyber Emergency Response Team in the US (ICS-CERT) included dams in its assessments along with other types of infrastructure such as chemical plants, manufacturing facilities, and wastewater treatment. According to one report, ICS-CERT had performed 98 assessments and recorded

94 instances of weak boundary protection of the control system which could facilitate unauthorized access. There were also incidences of unnecessary services, devices, and ports on control systems, as well as weak identification and authentication management. Furthermore, large and significant dams were considered to be at risk from unauthorized access.

4.2 Human Factors in an Example of Cyber Threats to Compromise Dam Operation

Cyber threats are viewed as a growing concern in the dams' community due to implications for public safety. Increasing vulnerability has been created due to facilities' previously manually operated components becoming more complex and supplemented with remote capabilities. As the number of connected technologies in a facility's control systems, such as in dams' increases, so does the cyberattack exposure of those systems. Automation has its benefits, such as efficiency and capturing real-time data and information, but it does also create new risks.

Opening the Flood Gates of a dam in the wrong time can lead to catastrophe. If this operation is carried out by a hacker; then such thing becomes reality more than fiction. In the scenarios developed for such occurrences, one hacker seeks to create significant disruption in opening of the flood gates at a dam. If any such scenario were to occur, it is likely to cause significant downstream flood damages in addition to public outcry. It is only natural then that the cyber security of important systems has gained lately special weight.

According to the report "Silent Cyber Scenario: Opening the Flood Gates", the cyber security of critical infrastructure, such as dams, has become a focal point in recent years. The report cites the event in 2013 when the control system at Bowman Avenue Dam in the United States was breached for about three weeks. The hacker obtained access to remote operation of the dam gates, which had fortunately been taken offline for maintenance [19].

Although the Bowman Avenue Dam is a small dam Figure 9, the manipulation of its gates by one hacker raised high concerns of such a possibility in lager dams. Hackers traced to Iran infiltrated the control system of this dam located just about 30 miles north of Manhattan; in 2013. The floodgate of the Bowman Avenue Dam is just 15 feet wide and two and a half feet tall, but cybersecurity experts say if the Iranians were able to access its control system, then they could likely get inside systems for more significant infrastructures, such as pipelines, mass transit systems and power. The incident itself passed without causing any damage because the structure was in "maintenance mode". But, if the hacker had been able to open the floodgate during a storm, then this could have caused nearby homes and businesses to flood.

The news of this incident brough the dam into the spotlights. In the words of Manhattan U.S attorney; the infiltration of the Bowman Avenue Dam represented a frightening new frontier in cybercrime. He also added, "we now live in a world where devastating attacks on our financial systems, our infrastructures and our way of life can be launched from anywhere in the world, with a click of a mouse".

Cyber security expert Joe Weiss commented on the incident by saying, "even if

local flooding is the worst that could have happened if the hacker opened the floodgate, the incident shows how vulnerable infrastructures are to such threats", adding ,"the control system for the Bowman Avenue Dam is likely similar to those for more significant structures and that the same identical problems can happen in power plants, refineries, pipelines, transportation and even in nuclear plants".

Figure 9: Downstream view of the Bowman Avenue Dam.

According to Weiss who maintained a database of "cyber incidents" involving control systems dating to the 1980s. Though not all of the 800 incidents were "malicious," he says, they have led to some 1,000 deaths. Ten of the overall incidents involved dams. He mentions that it is often that hydro facilities are in the middle of nowhere, and they are in many instances are unmanned, and so there is need for some sort of remote monitoring and remote control to avoid major problems. One such problem occurred at the Taum Sauk Hydroelectric Power Station in Missouri in 2005 which was described in this paper, when the failure of water-level gauges is believed to have caused water to overflow and part of a reservoir to collapse, which injured several people. The incident was the result of a control system and human multi failures, not a hacking or cyber-attack, but Weiss says: "It could have been done maliciously, and very easily" [20, 21].

The question of incursion on dams' safety by cyber means, whether to be considered as an armed attack threshold at which a State may take forceful action in self-defense or not, has received considerable study by International Law experts. In general, if the consequences of cyber operations targeting a State's infrastructure are destructive and injurious; then it is more likely that such cyber-attacks be considered the same as an armed attack. The approach of the Tallinn Manual on the International Law applicable to Cyber Warfare which was formulated between 2009 and 2012, considers that cyber actions that qualify as an armed attack open the door

to a forceful response, by either cyber or non-cyber means, pursuant to the law of self-defense, though this must be assessed on a case-by-case basis.
The US views is precisely the same. Harold Koh, the then-legal adviser at the US State Department, explained in 2012 that "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force." He noted that "commonly cited examples of cyber activity that would constitute a use of force include, for example, (i) operations that trigger a nuclear plant meltdown; (ii) operations that open a dam above a populated area causing destruction; or (iii) operations that disable air traffic control resulting in airplane crashes". Koh stated that "when assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues" [22].

4.3 Human Factors and the Hazards to Dams Created From Acts of War

Destruction of dams during times of war is one more source of concern to governments; this concern is reasonably justified since destruction of dams has been done during wars throughout history. Such destruction, however, took much greater dimensions in World War II with the objectives of inflicting maximum human losses in the civilian population, and paralyzing warring parties by disrupting the industrial production supporting the enemy's war effort. In the following, some cases are described when dams were the subject of war hostilities.

4.3.1 Bombing of the German Dams in World War II

In this case bombing raids were carried out by the British Royal Air Force (RAF) to destroy three dams in the Ruhr valley in Germany on the night of 16-17 May 1943 in what was called operation chastise. The dams were fiercely protected. Torpedo nets in the water stopped underwater attacks and anti-aircraft guns defended them against enemy bombers; these dams secured the water supply for much of the surrounding areas and industries. It was planned that the destruction of these dams in this region would cause massive disruption to the German war effort. The plan, however, required the development of a weapon capable of destroying these dams and converting the Lancaster type bomber aircraft to deliver it. The bomb was needed to be dropped from a height of 18m at a ground speed of 232 mph (374 kph). The bomb would spin forwards across the surface of the water before reaching the dam. Its residual spin would then drive the bomb down the wall of the dam before exploding at its base, Figures 10 and 11. The three main targets were the Möhne, Eder and Sorpe dams. The Möhne dam was a curved "gravity" 40 m high and 650 m long concrete dam, Figure 12. There were tree-covered hills around the reservoir, but any attacking aircraft would be exposed on the immediate approach. The Eder dam was of similar construction but was an even more challenging target. Its winding reservoir was bordered by steep hills. The only way to approach would be from the north. The Sorpe dam was a different type of dam and had a watertight concrete core 10 m wide. At each end of its reservoir, the land

rose steeply making the approach path of the attacking aircraft exceedingly difficult. The Möhne dam was attacked first at 12.28 am and was breached, Figure 13, then the Eder dam was next which in its turn collapsed at 1.52 am. Meanwhile, aircrafts from the two other waves bombed the Sorpe dam, but it remained intact.

The two direct bombs hits on the Möhne dam resulted in a breach around 76 m wide and 89 m deep. The destroyed dam poured around 330 million tons of water into the western Ruhr region. A torrent of water around 10 m high and travelling at around 24 km/h swept through the valleys of the Möhne and Ruhr rivers. A few mines were flooded; 11 small factories and 92 houses were destroyed, and 114 factories and 971 houses were damaged. The floods washed away about 25 roads, railways and bridges as the flood waters spread for around 80 km from the source. Estimates show that before 15 May 1943 steel production on the Ruhr was 1 million tons; this dropped to a quarter of that level after the raid.

Figure 10: View of the Lancaster bomber and the bomb to attack the German Dams [23].

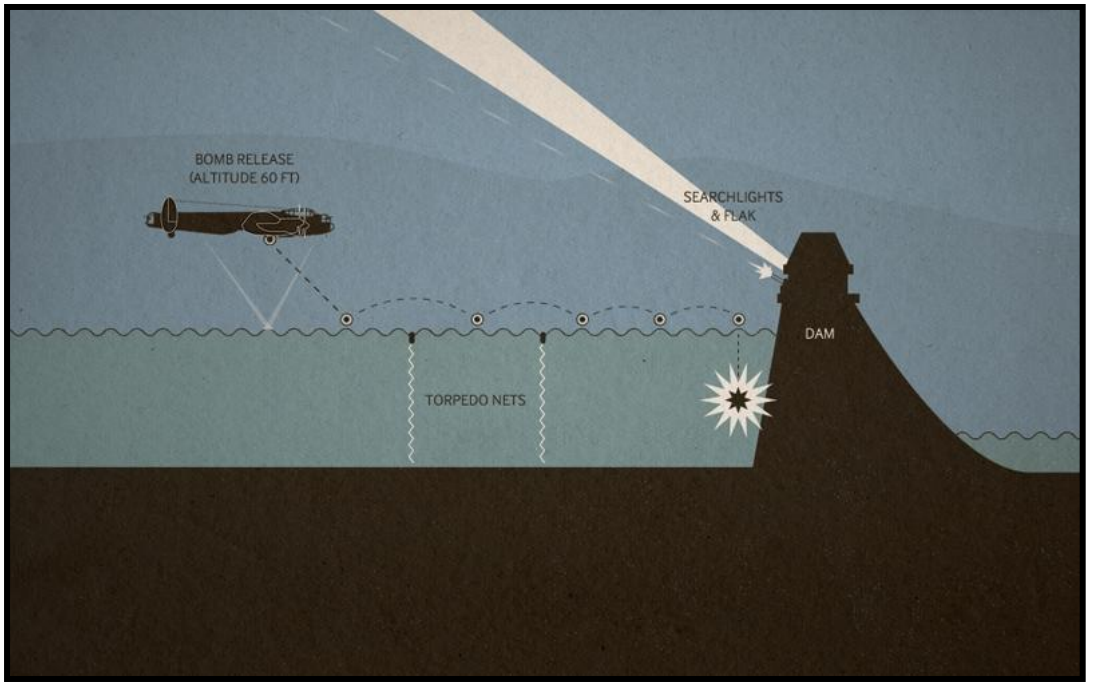

Figure 11: The visualized attack by the bouncing bomb on the German Dams [23].

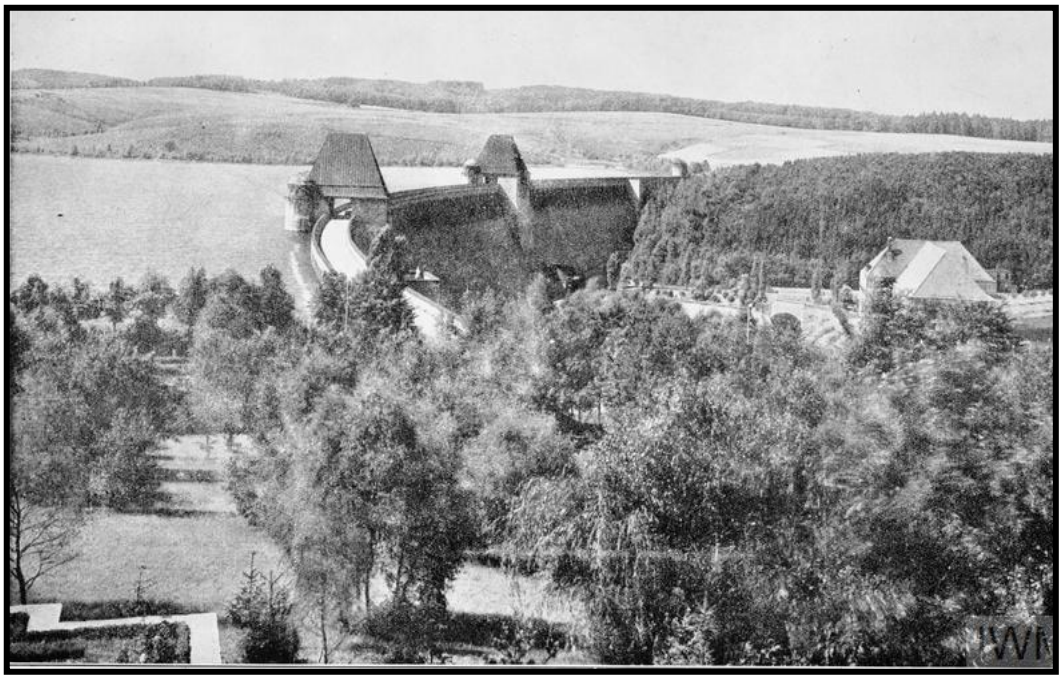

Figure 12: View of the Möhne dam [23].

In the case of Eder Dam, the main purpose of which was to act as a reservoir to keep the Weser and the Mittelland canal navigable during the summer months, the wave from the breach was not strong enough to result in significant damage by the time it hit the city of Kassel approximately 35 km downstream.

Figure 13: View of the Möhne dam breaching [23].

The greatest impact on the Ruhr armaments production was the loss of hydroelectric power. Two power stations, producing 5,100 kilowatts, associated with Möhne dam were destroyed and seven others were damaged. This resulted in a loss of electrical power in the factories and many households in the region for two weeks. In May 1943, coal production dropped by 400,000 tons which German sources attribute to the effects of the raid [24].

Although the raids were considered successful at the time many of the attacking airplanes were hit and crashed. Of the 133 aircrew that took part, 53 men were killed and three became prisoners of war.

On the ground, almost 1,300 people were killed in the resulting flooding, but the impact on industrial production was limited [23].

The principle of the dam buster bomb was described by its inventor Barnes Wallis in his 1942 paper "Spherical Bomb", as an attack in which a weapon would be bounced across water until it struck its target, then sink to explode underwater, much like a depth charge. Bouncing it across the surface would allow it to be aimed directly at its target while avoiding underwater defenses, as well as, some above the

surface, and such a weapon would take advantage of the "bubble pulse" effect typical of underwater explosions, greatly increasing its effectiveness, Figure 14.

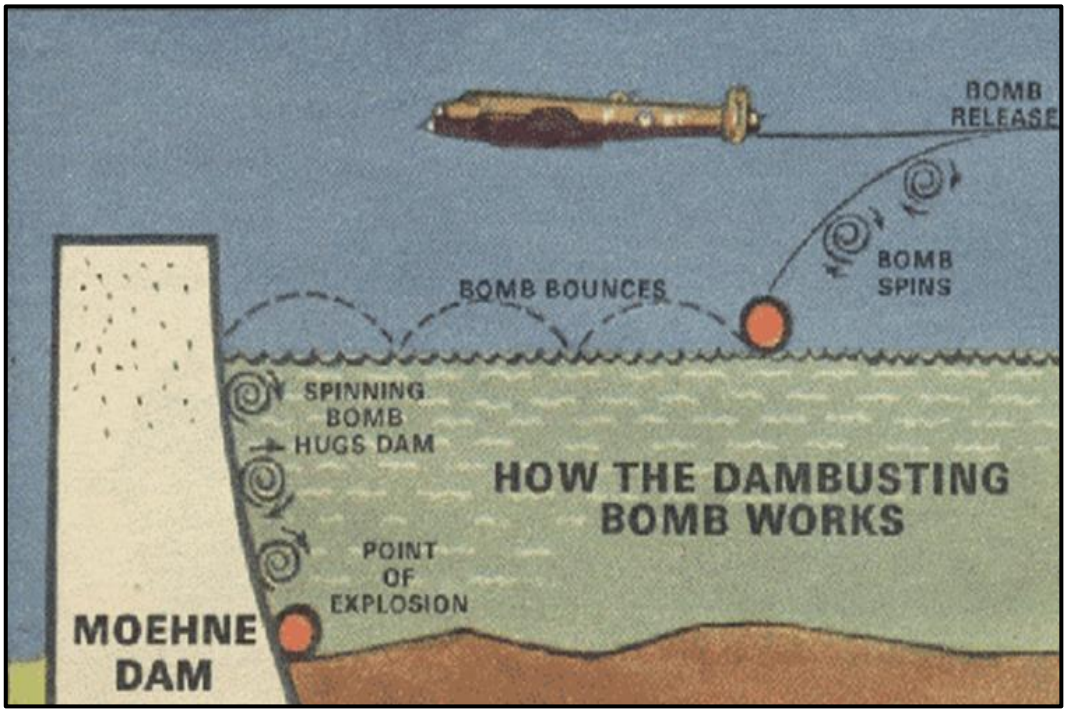

Figure 14: Bouncing bomb principle [25].

Wallis's paper identified suitable targets as hydro-electric dams and floating vessels moored in calm waters. The principle on which the bomb works were based on creating an earthquake impact on the dam it hits [26].

4.3.2 Blasting the Dnjeprostroj Dam

Another instance of targeting dams in wars is the blowing up of Dnieper Hydroelectric Station in the Ukraine: also known as Dnjeprostroj Dam; which is the largest hydroelectric power station on the Dnieper River. The station was built in two stages. Dnipro- HES-1 was originally built during 1927-32, but it was destroyed during World War II to make use of the river as a natural obstacle.

The strategically important dam and plant was dynamited by retreating Russian Army troops in 1941 after Germany's invasion of the Soviet Union. An account which described the aftermath of the Russians action went into details of how the explosion had flooded villages and settlements along the Dnieper River.

The tidal surge killed thousands of unsuspecting civilians, as well as Red Army officers who were crossing over the river. Then, it was partially dynamited again by retreating German troops in 1943. In the end, the dam suffered extensive damage, and the powerhouse hall was nearly destroyed. Both dam and station were rebuilt between 1944 and 1949. The Dnepr- HES-2 was built in 1969-80, which during the

2000s was modernized. Figure 15 shows the original dam under construction, and Figure 16 shows it after being damaged, while Figure 17 shows it after modernization [27].

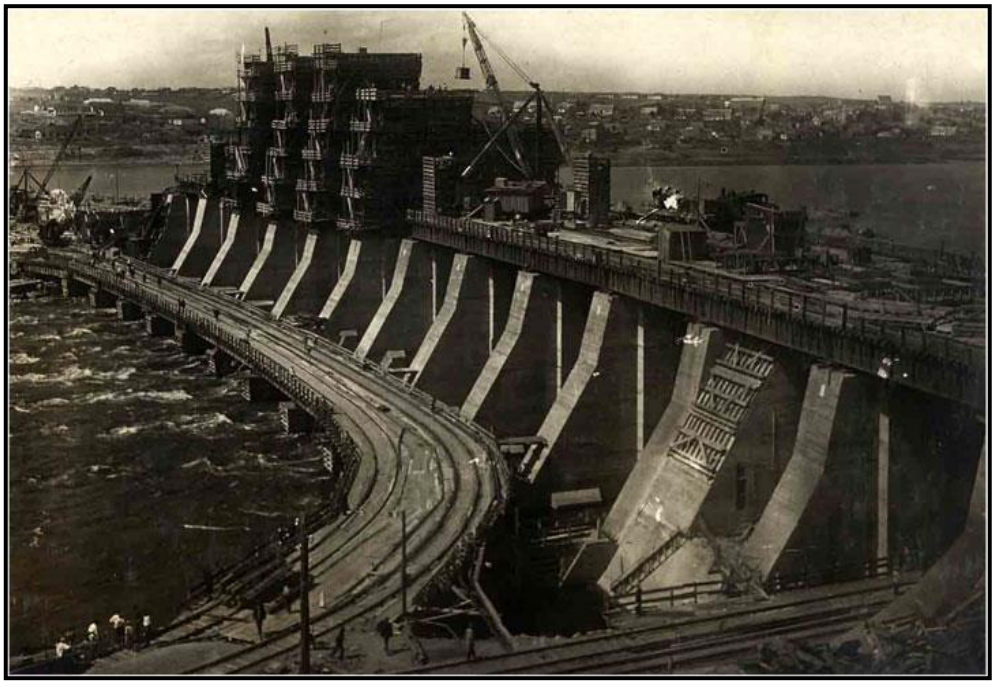

Figure 15: The dam under construction [27].

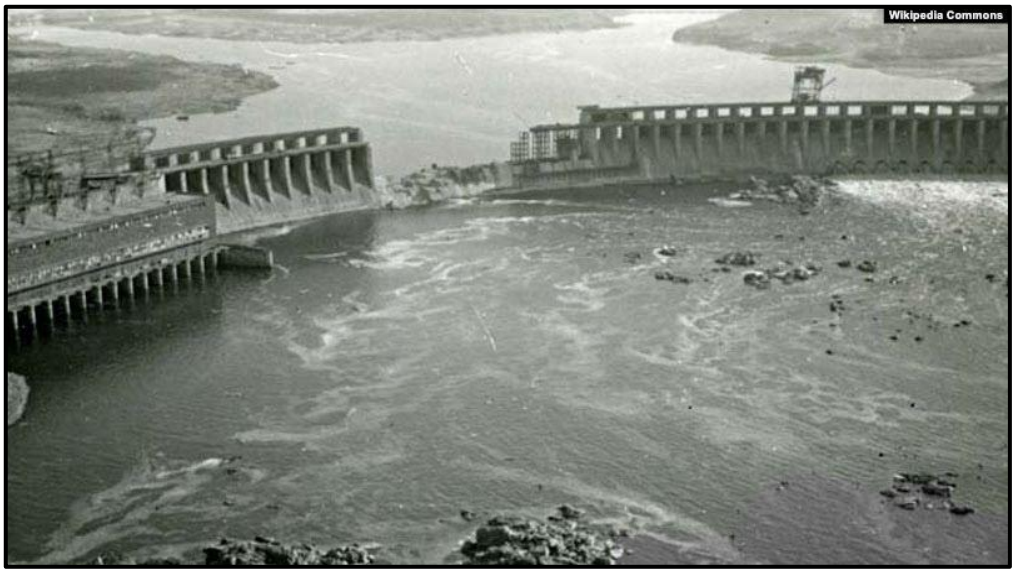

Figure 16: The dam after the incident [28].

Figure 17: The dam after modernization [27].

Since no official death toll was released at the time, the estimated number of victims varies widely. Most historians put it between 20,000 and 100,000, based on the number of people then living in the flooded areas [28].

4.3.3 Burguillo and Ordunte Dams Attacks

Burguillo and Ordunte concrete gravity dams were attacked and damaged by the Nationalist army in the Spanish civil war in 1937.

The Burguillo Dam near Avila, Figure 18 [29] is 91m high, which has a reservoir of 287.22 million cubic meter capacity. The second one is 56 m high Ordunte near Bilbao, Spain.

It was reported that a 2.5 ton charge was detonated in an inspection gallery at Ordunte. Some limited damage resulted. The dams were repaired in 1938–1939 [30].

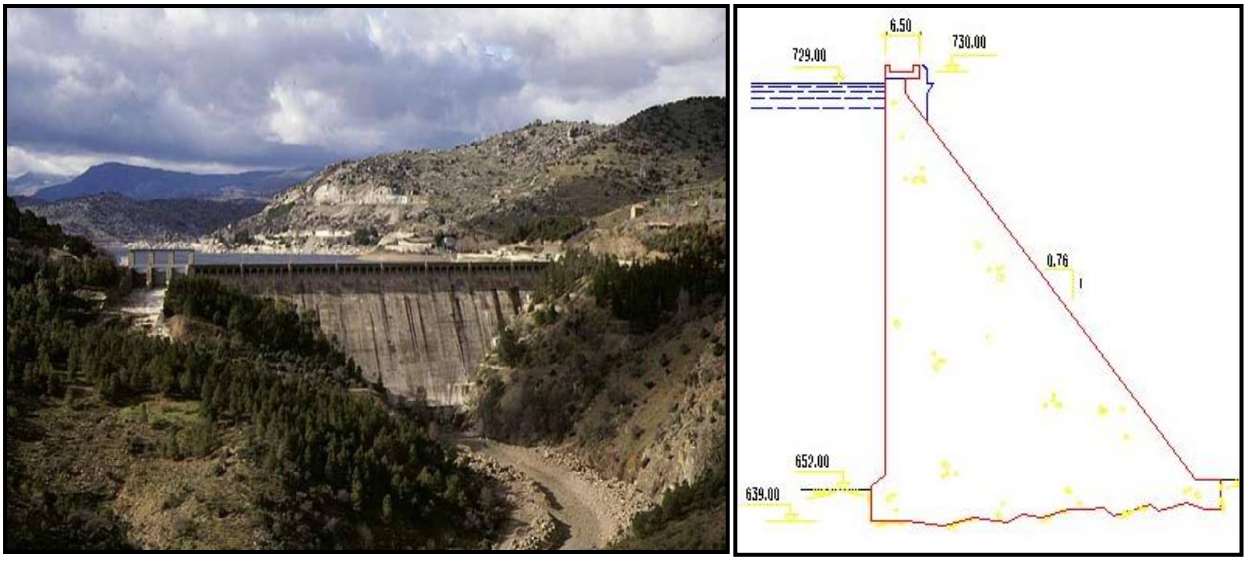

Figure 18: View and cross section of Burguillo Concrete Gravity Dam completed in 1913 [30].

4.3.4 Hwacheon Dam Attacks

From the Korean War, the example of the Hwacheon dam can be cited. This is a concrete gravity dam 81.5 m high, 435 m long and holds a reservoir of 1,018 million cubic meters of water. It is located on the North Han (Pukhan) River in Hwacheon County, Gangwon-do Province, South Korea. The dam was completed in 1944 as a primary source of electricity in southern Korea, and it also provides flood protection from North Korea's Imnam Dam upstream. It was the focal point of a raid during the Korean War. At midnight 8 April 1951, North Korea and Chinese forces released excess water from the dam's spillway which disabled five floating bridges of the United Nations Command downstream. On 9 April, the American forces were charged with the task of capturing the dam but failed. Between 16 and 21 April, Allies had secured the dam but were repelled by Chinese counterattack before being able to destroy the dam's floodgates. After an unsuccessful attempt to destroy the dam using heavy bombers, another raid was more successful on the 1st of May. The American use of aerial torpedoes was successful by dropping 2,000-pound torpedo bombs on the dam, puncturing one spillway gate, Figure 19 [31].

On 1st May 1951, US Air Group 19 assaulted the dam with eight Skyraiders attack bombers that were equipped with Mk 13 torpedoes and escorted by twelve corsairs fighter planes. Seven of eight torpedoes of 2,000 pound bombs struck the dam, and six exploded. The attack alleviated the dam as a flood threat, destroying one sluice gate and damaging several others [32]. This raid constitutes the last time globally that an aerial torpedo was used against a surface target, and was the only time torpedoes were used in the Korean War.

Figure 19: Hwacheon Dam being hit in the Korean War in 1951 [31, 32].

4.3.5 Peruća Dam

The blasting of the 63 m high earthfill Peruća Dam in Croatia in 1993 is the last example of these illustrations. The dam was constructed on Cetina River in 1958. The dam's reservoir active storage is 565 million cubic meters at the maximum operating water level at elevation 361.50 m (a.s.l.). The maximum reservoir flood level is 362.00 m (a.s.l.). The dam affects the Cetina flow regulation at the downstream power plants between Sinjsko Polje and the Adriatic considerably.

The Peruća Dam was greatly damaged during the Croatian War of Independence, when on January 28, 1993 the dam was blown up by Serbian/Yugoslav army forces. They mined it with 30 tons of explosives and detonated the charges with the intention of harming thousands of Croatian civilians downstream. The explosion caused heavy damage, but ultimately failed to demolish the dam. The Croatian communities in the Cetina valley were, nevertheless, in great danger of being flooded by water from Peruća Lake. The actions of an officer from the United Nations Protection Force (UNPROFOR) which was the first United Nations peacekeeping force in Croatia, Bosnia and Herzegovina during the Yugoslav Wars prevented the disaster at the Dam. Before the explosion, raised the spillway's gates were raised and reduced the level of water in the lake by four meters. This prevented total collapse of the dam, and engineers were quickly able to maintain the integrity of the dam. Subsequently, the Croatian forces intervened and recovered the dam and the surrounding area. On January 29, 1993 a small Croatian army team, supported by engineers previously employed in dam maintenance could get access to the main outlet valve which was stuck due to two years of neglect. Loaded with 700 tons of hydrostatic pressure on the valve, the engineers managed to refill the oil

in the hydraulic pumps and used an UNPROFOR engine to restart them. This allowed for the lake to finally drain into Cetina River at rate of 187m^3/sec [33, 34].

4.4 Human Factors and the Hazards to Dams From Terrorists Actions

4.4.1 General

Terrorism is defined as the acts of violence intentionally perpetrated on civilian non-combatants with the goal of furthering some ideological, religious or political objective. In the current national security environment, there is little question that terrorism is among the gravest of threats [35].

The importance of freshwater and water infrastructure to human and ecosystem health and to the smooth functioning of a commercial and industrial economy makes water and water systems targets for terrorism. The chance that terrorists will strike at water systems is real; indeed, there is a long history of such attacks [36].

Water infrastructures such as dams and water purification plants can be targeted directly causing flooding, or water can be contaminated through the introduction of poison or disease-causing agents, and in both cases, this can cause mass killing of people. This hazard has been recently recognized as one of the deadliest threats to dams' safety when used as either targets or tools of violence or intimidation by non-state actors. From recent history, some cases can be cited for using dams as a political tool. In one case reported by the ITAR-Tass News Agency; a threat was made on November 6th, 1998 by a guerrilla commander, Col. Makhmud Khudoberdyev, who threatened to blow up a dam in Tajikistan unless his demands were met. This rebel commander, in the northern part of the former Soviet Republic, threatened to blow up this particular dam and flood vast areas of Central Asia if the government did not meet his demands. "It will flood vast territories of Central Asia," Col.

Makhmud Khudoberdyev warned in a statement received by the ITAR-Tass news agency. He said his guerrillas had mined the dam on the Kairakkhum channel as a "deterrence measure." The dam's reservoir is large enough that it was referred to locally as a "sea". The government, which had no immediate reaction to the threat, said it had surrounded Khudoberdyev headquarters and recaptured Khodzhand, a city in the north of this small, impoverished nation.

Dozens of people were killed in the recent conflict there. The rebels had opposed the previous peace agreement ending the country's six-year-old civil war and wanted fresh elections [37].

In other case rebels from the Democratic Republic of Congo carried out attacks in 1998 on Inga Dam during efforts to topple President Kabila, disrupting electricity supplies from the dam and water supplies to Kinshasa, Congo (refer to case No. 194 in [38]). The rebels overran Inga hydroelectric dam in the early phase of their offensive on the capital Kinshasa from bases in the southwest of the country. Since that time, they repeatedly interrupted the power supply to the capital, leading to the disruption of running water supplies to the population. Medical services and supplies were also severely affected by the outage. Following the recent intervention on the government side of forces from Angola and Zimbabwe, the

military balance dramatically shifted in favor of loyalist forces and their allies. According to reports in an Angolan government-owned newspaper, rebels besieged in the dam area threatened to destroy the electricity installations if they were not granted safe passage out of there [39].

To shed more light on this hazard two more cases are presented in the following.

4.4.2 The case of Zgorigrad and Vratsa dam

In a case of sabotage which was suspected as a terrorist action was that of Zgorigrad and Vratsa mining dam in Bulgaria in 1966. This dam was an earthfill tailing dam with a puddle concrete membrane impounding a sediment basin for lead and zinc mine called Mir located uphill of the village of Zgorigrad near Vratsa.

The breaching and collapse of the dam created 4.6 m high flood wave through the towns of Zgorigrad and Vratsa. Reports indicated that as many as 600 people perished in this disaster [40, 41, 42].

The catastrophe of Zgorigrad is one of the worst disasters caused by the failure of tailings dams worldwide. On 1st May 1966, the failure of this tailings dam gave rise to a 450,000 cubic meter of mud flow, which ran for a distance of 6 km as far as the town of Vratza and caused the loss of many hundreds of lives, as well as vast material and environmental destruction. The slurry and water contained poisonous chemical elements [43, 44].

Quoting from another report in Bulgarian language, it stated the following:

"*Officially, the Communist authorities at that time announced only about 100 deaths, but later it became clear that the victims of the incident were over 500 (there are reports of 118 corpses unidentifiable, of which 4 children), injured 2000, more than 150 houses destroyed, 300 families are left without a home, and the roofs of 1000 houses are taken from the elements".*

The same report contains some photographs taken in the aftermath of the failure. Remains of the dam's outlets which take the water out from the sedimentation basin after the event is presented in Figure 20.

While Figure 21 shows the people of Zgorigrad cleaning the city streets from the metallic mud that covered everywhere, and Figure 22 illustrates the extent of ecological damage inflicted by the disaster on the downstream area and the official work to remove as much as possible of the mud [45].

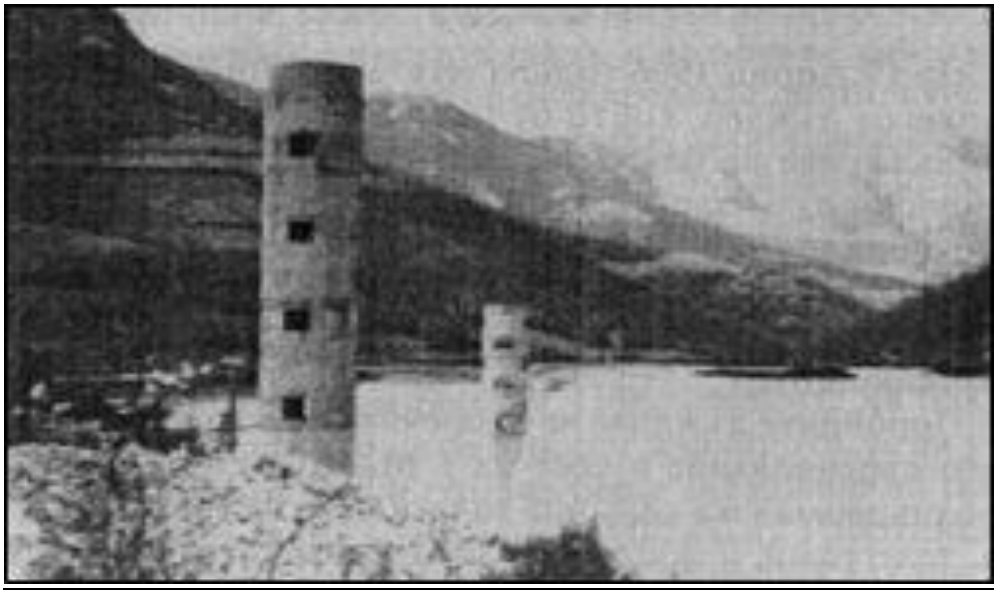

Figure 20: Photograph showing outlet spillways of the sedimentation basin [45].

Figure 21: Cleaning of Zgorigrad streets from the toxic mud [45].

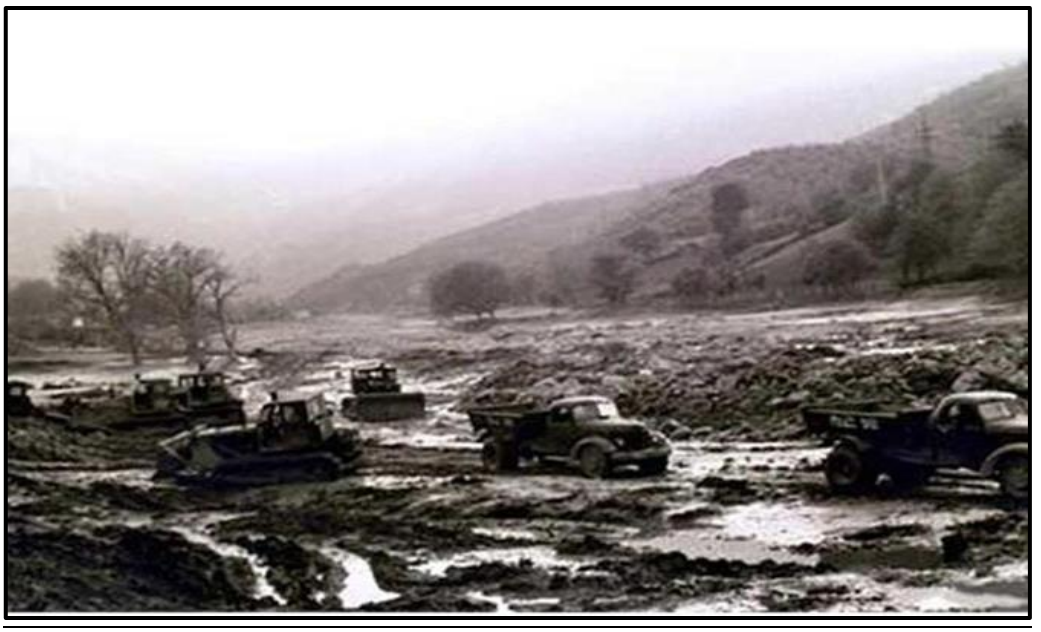

Figure 22: Cleaning operations in the flooded downstream Area [45].

4.4.3 The Rise of ISIS and the Threats it Presented to Dams in Iraq

The rise of the Islamic State in Iraq (ISIS), known also in the media as the Islamic state in Iraq and the Levant (ISIL), and its control of vast swathes of land in Iraq and Syria in 2014, can be considered as the most dramatic event in the recent history of the two countries and in the world. This fundamentalist fanatical religious group may be considered as the most radical group so far in modern history seeking to change the values and systems in the Islamic world. Therefore, establishing their brand of governance through the use of violence and targeting the population to force them into submission, and at the same time destroying most of the existing economic and social infrastructures in an attempt to weaken the authority of government(s).In their ways and methods, they used water as a weapon. One of the earliest examples was their seizure of Fallujah Barrage on the Euphrates River. The dam helps distribute water from the Euphrates River on its course through the western province of Anbar, and is located some 5 km south of Falluja town some 70 km (44 miles) west of Baghdad, the town which was overran by the militants early in their campaign. Early February 2014, ISIL took control of the Nuaimiya area where the dam is located, and began fortifying their positions with concrete blast walls and sand bags. Early in April of the same year, the militants closed eight of the dam's 10 gates flooding land upstream and reducing water levels in Iraq's southern provinces through which the Euphrates flows before emptying into the Gulf. In the following week, the militants re-opened five of the dam's gates to relieve some pressure, fearing their strategy would backfire by flooding their own stronghold of Falluja. The decline of water levels in the Euphrates also led to electric power shortages in towns south of Baghdad, which rely on steam-powered

generators that depend entirely on water levels. A spokesman for the Ministry of Electricity said the power supply from Musayab power station had decreased to 90 megawatts from 170 megawatts. Government officials and advisers warned that ongoing closure of the dam could affect irrigation of farms in many southern provinces that depend on the Euphrates Rvier, including Hilla, Karbala, Najaf and Diwaniya [46].

In June 2014, fighters with the Islamic State in Iraq and Syria were advancing on the Euphrates River towards the Haditha Dam, the second largest in Iraq; located 120 miles (240 km) north west of Baghdad and the second-largest in Iraq. This action raised the possibility of catastrophic damage and flooding if they could take control of the dam. They already reached Burwana town, on the eastern side of Haditha town; six kilometers south of the dam site, and government forces were fighting to halt their advance. At one point, alarmed army officer told employees to stay inside and be prepared to open the dam's floodgates if ordered to flood the town and villages around. This would not be the first time that dams have figured in the conflict. In April, when ISIS fighters seized the Falluja Dam. They opened the gates, flooding crops all the way south to the city of Najaf. The water at one point washed east as well, almost reaching Abu Ghraib, close to Baghdad [47]. The security forces repelled ISIS fighters from Haditha later on in July [48].

In the same way ISIS had captured Ramadi Barrage north of the Iraqi city of Ramadi upstream from Falluja town and closed off its gates cutting water supplies to pro-government towns downstream and making it easier for its fighters to attack forces loyal to Baghdad. ISIS militants were opening only two or three of the dam's 26 gates for brief periods daily. This move was to prevent river water overflowing from ISIS' side of the dam, and also to allow some water to flow downstream toward ISIS-held Falluja. Water level in the Euphrates River was so low that the river could be walked across, making it easier for ISIS militants to cross and attack the pro-government town of Khalidiyah as well as the large security forces base at Habbaniyah. The level of the Euphrates River dropped by one meter near Amiriyat al-Falluja [49].

Similarly, the area around the Thartar Dam and the dam site itself near Falluja town, 98 km west of Baghdad, were the sites of many fierce battles between ISIS fighters and government forces. The main dam controls the flow from Lake Tharthar reservoir to the main feeder canal returning the flow to augment the Euphrates River flow in summer, and branching to do the same thing to the Tigris River flow. The militants could use the dam and the two other regulators on the feeder canal to inflict damage by flooding areas in Bagdad and Falluja. In one occasions, a U.S. official said intelligence reports suggest the extremists had opened at least one of the dam's gates, although darkness has hampered efforts to determine how much flooding had resulted. All this led to many offensives to retake the dam and the area around it. In one of these operations, an army general was among the casualties, and 40 soldiers were taken captive by the militants [50].

One of the failed attempts of the terrorist group to capture a major dam and use it as a weapon of mass destruction was their attack in February 2015 on Adhaim Dam

located 133 km northeast of Bagdad on Al-Adhaim River; a tributary of the Tigris River. At least 18 people, including 14 militants, were killed and 23 others injured as Iraqi security forces repelled ISIS. The attack occurred around Saturday midnight when dozens of ISIS militants, including suicide bombers, attacked the dam site but retreated after four hours of clashes [51].

Out of all these cases, the occupation of Mosul Dam site in August 2014 remains probably as the worst of all the other mentioned incidents.

Mosul Dam is located in north of Iraq on the Tigris River just 40 km north of the city of Mosul. It is the largest dam in Iraq, and it controls the Tigris River flow on its entry from Turkey with an active storage of 11.11 billion cubic meters of water. The fall of Mosul city to the insurgents between 4–10 June 2014 marked the beginning of a bloody saga in and around the city and opened the way to capture of Mosul dam on the 8th August 2014. The world was then holding its breath and waiting to what could have been the worst and most destructive man- made flood in history. This situation prompted; however, a swift and determined action to liberate the dam on the 18th of the same month from ISIS hands by the Iraqi forces and Kurdish Peshmerga supported by heavy air strikes carried out by the US air force [52, 53].

The dam site was taken back, and it was saved from serious damage, but this case taught everybody a lesson to secure this type of structures at any cost. As a target with special important Mosul Dam was tagged by the international media as a weapon of mass destruction. It was fortunate that the terrorist group did not have enough time to plan and execute demolition acts, and the reservoir was at its lowest level at the time.

One more reason for abstaining from this could have been that ISIS did not wish to flood the city of Mosul which they had already occupied and which they considered as a great prize and the second capital of their Islamic State.

This situation led; however, to suspend the maintenance grouting operations that had continued for 30 years for more than one year. The continuous grouting operations were considered as the only possible mean to secure the dam against failure due to the continuous dissolution of gypsum in its foundation. In fact, an intensive study based on field measurements was performed during 2015 by the American Army Corps of Engineers who showed that the foundation was deteriorating at a very fast rate in view of halting of the grouting works; a case which led finally intensive efforts to continue the grouting operations that were resumed in the first quarter of 2016 [52].

5. Summary Points and Lessons Learned

Although dams' safety is characteristic of design, construction and host of many other various elements of pure technical nature, dams' safety is also influenced by "Human Factors" which can become important issues in this matter. Proper management based on good knowledge, and expertise can mitigate safety levels thus reflect positively on dam conditions and reduce a safety hazard to a minimum. However, variety of these human factors can also impair this safety, which reflects the negative aspects of the "Human Factor". In this paper, we have tried to distinguish between two types of accidents involving dams which are related to human factors. The first are "Normal" accidents, which are related to unintentional mistakes and errors committed by site operators or remote controllers in operating one or more dams as a system. The second are what we have called the "Extraordinary" accidents; meaning they are caused by human actions for purposely destabilizing dams after thoughtful and carefully meditated decision making process. These are manifested in sabotage, terrorism attacks and acts of war.

Normal human errors and mistakes which lead to magnifying dam safety risks can be attributed to; personnel ignorance or negligence, or even still to overconfidence, insufficiently trained personnel or personnel that are unaware of risks and their lack of real time information ,which can exasperate the risks. The complexity of situations and lack of clear instructions may lead to risky situations also, and generally, human limitations due to fatigue, emotions, indifference and over stress can cause such dangerous conditions.

Lessons learned from such accidents due to human failings are, to have only highly trained personnel in charge of operation of dams, to simplify operation procedures as much as possible and provide clear instructions and operation manuals, in addition to following up all the instrumentation measurements and make sure of the good working conditions of the respective instruments by constant inspections.

In modern procedures, ITC applications have been used in operation of various systems, including dams. Decisions in many instances are made depending on the Supervision, Control and Data Acquisition (SCADA) systems without directly seeing the structure(s). Pitfalls in control software may appear in untried situations; similarly, an unexpected error in one element of the software can cause dangerous conditions. In such cases, alarm signals might be wrongly interpreted, or operation commands are not correctly received. Complexity of situations in site or remotely controlled system of dams can be exasperated by IT system failures. All such things can happen within the normal technological routines or to say normal human factors. Lessons learned from dam incidents of such nature necessitate taking all precautions to have fool proof software with capacity for detecting and correcting errors, to have feedback capabilities and avoid consequences of IT system failure by having more than one channel for communication.

The use of modern technologies in controlling the direct operation of one dam or the remote control of a system of dams can lead in some cases into quite dangerous situations if these systems are not well guarded against external intrusion. This may

result from cyber-attacks aimed at disrupting the normal operation of the system and leading to substantial deviation from the operational state as per design intents. Creating such dangerous situations can result from accidental or intentional misuse of the (ICT) technologies used for the dam(s) control, or can be a consequence of hackers' action infiltrating the system through loop holes which the owner was not been aware of.

Lessons learned are; to limit the number of the (ICS) users who have administrator access and; to reduce the extensive number of group accounts and limit that to the bare necessary; to make sure of the compliance with password policies by authorized users; and to remove inactive system administrators accounts. All these actions are to be done for stopping hackers who may have malicious intentions from creeping into the system. Moreover, it may be necessary that personnel with elevated system privileges should be subjected to complete and more rigorous background investigations. On top of this the mental health of authorizes users should be given enough scrutiny, and they should pass thorough psychological examination to bar entrance to the system to those which might have psychological disorders such as suicidal inclinations. This may be based on incidents, which have occurred in other fields activities and reminds us of Germanwings flight 9525 on 24th March 2015 when the 28-year co-pilot Andreas Lubitz had used the flight management system voluntarily to start the fatal rapid descent of the aircraft and the eventual crash into the French Alps killing himself and the 150 passengers and the crew on board [53].

In more willful human actions aiming at dams' safety and causing "Extraordinary" incidents are acts of war, terrorist attacks; and sabotage work.

Destruction of dams during times of war has been one big source of concern to governments which stems from the many cases of dams' destruction in wars throughout history. Water resource systems including dams were targeted by combatants, including nations or states, and the intentions were to use water as a weapon to occupy an area or to bar the enemy from that area. Added to these in recent wars, the other objectives were inflicting maximum human losses, in spite of the 1949 UN Geneva convention, ratified in1977 on the protection of civilians in times of war [54]. Other intentions were paralyzing the enemy by disrupting his industrial production supporting the war effort as in World War II. This was also done in many late instances as in the 1991 Gulf war and the occupation of Iraq war in 2003. These acts were done by the same countries who claim their advocation of human rights and upholding the International Law. But regrettably, these cases show clearly that human greed and want for vengeance have no limits.

Lessons learned as they became clear are, however; that using dams as tools in wars affects, mostly innocent civilians and cannot reverse the outcome of any war. Governments should abstain from such acts under any pretext or excuse, and all shall come to agree that these acts should be covered by the international humanitarian law, The Law of The Hague, which addresses the various types of weapons and their permissible uses, as well as the behavior of combatants during hostilities; in addition to the Geneva rules, which, deal with the humanitarian

treatment of the victims. Some of the underlying principles of the laws of war referred to are also the laws of armed conflict in a broader sense; that is the wanton destruction of human life, and property is prohibited.

Terrorist and saboteurs' actions, as we all know, have posed in late times another source of concern over dams' safety. The terrorist and saboteur's objectives have been to hold innocent civilian populations as hostages to force the government into submission to their political agendas using various means, including taking hold of dams. It is also clear from their actions and mentality that human madness sometimes goes further to even self-destruction.

In the present atmosphere of expanding use of the Media, terrorists and terrorist groups have also exploited the internet and social media not only to commit terrorist acts, but also to facilitate a wide range of terrorist activities, including incitement, radicalization, recruitment, training, planning, collection of information, communications, preparation, and financing [57].

As for putting an end to these follies, lessons learned are: Governments must work hard to eliminate the root causes which can emanate from social injustice or from fanatical religious ideologies; Governments shall, therefore, improve theirs record on human rights, improve living conditions and upgrade their education systems to match up with the challenges presented; Governments, moreover, are required to take extra care in the physical protection of dams and water resources infra structures and avoid any lax in their security. Finally, Governments should intensify and accelerate the exchange of operational information concerning the use of ICT systems by terrorist groups denying them any abuse of these systems.

References

[1] Perrow, C. (1999). Normal accidents: Living with high- risk technologies. Princeton University Press, N.J. https://openlibrary.org/books/OL15489746M/Normal_accidents.

[2] Holden, J. R. (2009). People or systems? To blame is human. The fix is to engineer. Professional safety, Volume:54, Issue:12, pp. 34-41. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3115647/ https://academic.microsoft.com/paper/2408263965/citedby/search?q=People%20or%20systems%3F%20To%20blame%20is%20human.%20The%20fix%20is%20to%20engineer.&qe=RId%253D2408263965&f=&orderBy=0

[3] Irfan, A. (2020). Lessons Learned: Dam Incidents and Failures can Fundamentally be Attributed to Human Factors. Case Studies, Association of States Dam Safety Officials, Website page accessed on 19th April 2020. https://damfailures.org/lessons-learned/dam-incidents-and-failures-can-fundamentally-be-attributed-to-human-factors/

[4] Komey, A., Qianl Deng, Q., Baecher, G. B, Zielinski, P. A. and Atkinson, T. (2015). System Reliability of Flow Control in Dam Safety. 12th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP12 Vancouver, Canada, July 12-15, 2015, uploaded online on 16 December 2015. https://www.goldsim.com/downloads/technicalpapers/System_Reliability_Dams.pdf

[5] Lempériére, F. (2017). Dams and Floods. Science direct, Engineering Vol. Issue 1, February 2017, pp.144-149. https://www.sciencedirect.com/science/article/pii/S2095809917301571.

[6] Vogelm, A. (2001). Safety Risk, Reliability-Trends in Engineering. Proceedings of the International Conference on Safety, Risk, Reliability-Trends in Engineering Malta 2001, downloaded from author CD- ROM: More information of the conference is found on the following link; https://heyblom.websites.xs4all.nl/website/newsletter/9903/lc.pdf

[7] Wikimedia (2020). Dibis Dam. From Wikipedia, accessed on April 19th 2020 https://wikivisually.com/wiki/Dibis_Dam

[8] USBR (2015). Final Environmental Assessment: Nimbus Dam Radial Gates Maintenance Project. Managing Water in the West. May 2015 https://www.usbr.gov/mp/nepa/includes/documentShow.php?Doc_ID=22106

[9] Downing, J. (2006). Dam's failed sensor caused water gush. American River Parkway Preservation Society Blog, February 7th, 2006. https://parkwayblog.blogspot.com/2006/02/nimibus-flood-gate-opens-accidentally.html

[10] Wikipedia (2020). Taum Sauk Hydroelectric Power Station. The free encyclopedia. Accessed on 21st April 2020. https://en.wikipedia.org/wiki/Taum_Sauk_Hydroelectric_Power_Station

[11] Rogers, D. J., Watkins, C. M. and Chung, J. W. (2010). The 2005 Upper Taum Sauk Dam Failure: A Case History. Environmental and Engineering Geoscience (2010) 16 (3): 257–289. https://pubs.geoscienceworld.org/aeg/eeg/article-abstract/16/3/257/60396/The-2005-Upper-Taum-Sauk-Dam-Failure-A-Case?redirectedFrom=fulltext

[12] Rogers, D. J. and Watkins, C. M. (2008). Overview of the Taum Sauk Pumped Storage Power Plant Upper Reservoir Failure, Reynolds County, MO. 6th International Conference on Case Histories in Geotechnical Engineering, Arlington, VA, 11- 16 August, 2008 http://web.mst.edu/~rogersda/dams/2_43_Rogers.pdf

[13] Regan, P. (2010). Dam s as Systems-A Holistic Approach to Dam Safety. Collaborative Management of Integrated Watersheds 30th Annual USSD Conference Sacramento, California, April 12-16, 2010. https://www.researchgate.net/publication/286383843_DAMS_AS_SYSTEMS_-_A_HOLISTIC_APPROACH_TO_DAM_SAFETY

[14] King, W. B., Calcagno, F., Evans, J. H., Gross, E., Lovullo, T. J., Peters, M., Richards, K., Shannon, P. and Strat T. (2010). Report of Findings on the Overtopping and Embankment Breach of the Upper Dam; Taum Sauk Pumped Storage Project. FERC Taum Sauk Investigation Team April 28 2006. https://www.researchgate.net/publication/275837940_The_2005_upper_Taum_Sauk_Dam_failure_A_case_history

[15] FERC Taum Sauk Investigation Team (n.d). Executive Summary- Report of Findings". https://ferc.gov/industries/hydropower/safety/projects/taum-sauk/staff-rpt/ex-sum.pdf

[16] Association of State Dam Safety Officials, (2020). Case Study: Taum Sauk Dam (Missouri, 2005). Lessons Learned From Dam Incidents and Failures, Blog Page accessed on 21st April 2020. https://damfailures.org/case-study/taum-sauk-dam-missouri-2005/

[17] War is Boring Blog (2014). Dam Warfare: Floods as weapons, from ancient times until Iraq today. Published online on July, 20th, 2014, Accessed on 22nd April 2020 https://medium.com/war-is-boring/dam-warfare 3da6ee24518a

[18] Office of Inspection General (2017). U.S Bureau of Reclamation Selected Hydropower Dams at increased Risk from Insider Threats. U.S Department of the Interior. Report No.: 2017-ITA-023 June 2018. https://www.doioig.gov/sites/doioig.gov/files/FinalEvaluation_ICSDams_Public.pdf.

[19] Honea, M., Yamamoto Y., Laux J., Guiliano, C. and Megan Hart, M. (2019). Silent Cyber Scenario: Opening the Flood Gates. October 2018. Compilation of the report by Water Power and Dam Construction Journal under the title "Hydropower facilities: vulnerability to cyberattacks". Published on 20th

March 2019. https://www.waterpowermagazine.com/features/featureunder-cyber-attack-7051600/
[20] Kunter, M. (2016). Alleged Dam Hacking Raises Fears of Cyber Threats to Infrastructures. Newsweek Magazine on 30th March 2016. https://www.newsweek.com/cyber-attack-rye-dam-iran-441940
[21] Thomson, M. (2016). Iranian Cyber Attack on New York Dam Shows Future of War. Time Magazine on 24th March 2016. https://time.com/4270728/iran-cyber-attack-dam-fbi/
[22] Allen, C. (2016). Was the Cyber Attack on a Dam in New York an Armed Attack. Us Government, Department of Defense 8th January 2016. https://www.justsecurity.org/28720/cyber-attack-dam-armed-attack/
[23] Masson, A. (2018). The Incredible Story of the Dam Busters Raid. The Imperial War Museum (IWM) website, January 5th 2018. https://www.iwm.org.uk/history/the-incredible-story-of-the-dambusters-raid
[24] Wikipedia (2020). Operation Chastise. Accessed on 24th April 2020. https://en.wikipedia.org/wiki/Operation_Chastise#Bomb_damage_assessment
[25] 1001 Crash.com. (2020). Lessons learned from aviation safety. Accessed on 24th April 2020. https://www.1001crash.com/index-page-Dam_Busters-lg-2.html
[26] Wikipedia (2020). Bouncing Bomb. Accessed on 24th April 2020. https://en.wikipedia.org/wiki/Bouncing_bomb
[27] Wikipedia (2020). Dnieper Hydroelectric station. Accessed on 24th April 2020 https://en.wikipedia.org/wiki/Dnieper_Hydroelectric_Station
[28] Moroz, D. (2013). Ukrainian Activists Draw Attention to Little Known WWII Tragedy. Radiolibirty, 23rd August 2013. https://www.rferl.org/a/european-remembrance-day-ukraine-little-known-ww2-tragedy/25083847.html
[29] Data Iagua (2020). Presda de Burguillo, EL. Web Page accessed on 24th April 2020 https://www.iagua.es/data/infraestructuras/presas/burguillo
Water Conflicts Chronology, (1937). "Dams Attacked in Spain Civil War, 1937".
Data Base accessed on 24th April 2020. http://worldwater.org/conflict/list/
[30] Hallon, R. (1986). The Naval Air War in Korea. Pp.120-121, University of Alabama Press, 1986. https://books.google.se/books?id=TLVnjOU1lf4C&pg=PA121&dq=Hwachon+dam+attack&hl=en&ei=fDU7TvOyL8jMmAXtjunnAg&sa=X&oi=book_result&ct=result&redir_esc=y#v=onepage&q=Hwachon%20dam%20attack&f=false.
[31] Wikipedia (2020). Peruca Lake. Web Page accessed on 25th April 2020. https://en.wikipedia.org/wiki/Peru%C4%87a_Lake
[32] HEP (2020). Eighteen years since the attempt to demolish Peruća Dam https://www.hep.hr/news/eighteen-years-since-the-attempt-to-demolish-peruca-dam/2864

[33] Borum, R. (2004). Psychology of Terrorism. Tampa, University of South Florida, 2004 https://www.ncjrs.gov/pdffiles1/nij/grants/208552.pdf
[34] Gleick, P. H. (2006). Water and Terrorism. Water Policy- Journal of the World Water Council, Volume 8, Issue 6, pp.481-503. https://pacinst.org/wp-content/uploads/2006/08/water_and_terrorism_2006.pdf
[35] World Rivers Review (WRR) (1998). Dangerous Dams: Tajikistan.. International Rivers Network, Vol.13, Issue 6: p.13. Berkeley, California: https://www.internationalrivers.org/sites/default/files/attached-files/wrr.v13.n6.pdf
[36] Pacific Institute (2020). Water Conflict Chronology. The world information on the world's Fresh Water Resources. Case No. 194. http://www.worldwater.org/conflict/map/
[37] Human Right Watch (1998). Human Rights Watch Condemns Civilian Killing by Congo Rebels. Human Right Watch International Justice. https://www.hrw.org/news/1998/08/27/human-rights-watch-condemns-civilian-killings-congo-rebels
[38] Hughes, A.K. (1981). The Erosion Resistance of Compacted Clay Fill in Relation to Embankment. PhD thesis, Vol.2, p.402, University of New Castle upon Tyne. Department of Civil Engineering1981 https://theses.ncl.ac.uk/jspui/handle/10443/1118
[39] Wikipedia (2020). Dam Failure - List of Major Dam Failures. Accessed on 26th April 2020. https://en.wikipedia.org/wiki/Dam_failure
[40] Clean River Trust (2016). Bulgarien Tailings Dam Failure. Accessed on 26th April 2020. https://www.cleanriverstrust.co.uk/bulgarian-tailings-dam-failure/
[41] Nickolova, D. (2006). Photographer's note on Vratsa dam failure. Trek Earth Photography, 2006-9-1. Webpage accessed on 9th July 2018. https://www.trekearth.com/gallery/Europe/Bulgaria/West/Vratsa/Sgorigrad/photo928141.htm
[42] World information Service on Energy (2018). Chronology of major tailing dam failures. Table compiled by WISE Uranium Project, last updated 15 June 2018 Accessed on 26th April 2020 http://www.wise-uranium.org/mdaf.html
[43] Web Page Zgorigrad (n.d.). Zgorigrad 1966 crash (In Bulgarian). Accessed on 26th April 2020. https://sgorigrad.com/%d0%b8%d1%81%d1%82%d0%be%d1%80%d0%b8%d1%8f-%d0%b7%d0%b3%d0%be%d1%80%d0%b8%d0%b3%d1%80%d0%b0%d0%b4/#tragedy1966.
[44] Rasheed, A., Raheem Salman, R., Coles, I. and Evans, C. (2014). Iraq insurgents use water as weapon after seizing dam. Reuters. https://www.reuters.com/article/us-iraq-security/iraq-insurgents-use-water-as-weapon-after-seizing-dam-idUSBREA3A0Q020140411?utm_source=Circle+of+Blue+WaterNews+%26+Alerts&utm_campaign=ede331b06d-

RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_c1265b6ed7-ede331b06d-250657157

[45] Rubin, A. J. and Rod Nordland, R. (2014). Sunni Militants Advance Toward Large Iraqi Dam. New York Times, June 25, 2014. https://www.nytimes.com/2014/06/26/world/middleeast/isis-iraq.html

[46] Itar, T. (2014). Security forces continue battles with insurgent groups in Iraq. Baghdad, 13July 2014. http://www.derechos.org/nizkor/iraq/doc/irq340.html

[47] Alkhshali, H. and Smith-Spark, L. (2015). ISIS fighters close Ramadi dam gates, cut off water to loyalist towns. CNN June 4, 2015. https://edition.cnn.com/2015/06/04/middleeast/iraq-isis-ramadi/index.html

[48] Alwan, A. (2015). Islamic State seizes dam, kills Iraqi general and more than 100 soldiers. The Sunday Morning Herald, April 26, 2015. https://www.smh.com.au/world/islamic-state-seizes-dam-kills-iraqi-general-and-more-than-100-soldiers-20150426-1mtcdg.html

[49] Business Standard (2015). 18 killed as Iraqi forces repel IS attack. 15th February 2015. Indo Asian News Agency (IANS). https://www.business-standard.com/article/news-ians/18-killed-as-iraqi-forces-repel-is-attack-115021500581_1.html

[50] Reuters (2014). Mosul Dam: U.S. Airstrikes Pound ISIS Militants Holding Key Iraqi Facility. Based on BBC news report, August 17th, 2014. https://www.ibtimes.com/mosul-dam-us-airstrikes-pound-isis-militants-holding-key-iraqi-facility-1660630?rel=rel2

[51] Kreiter, M. (2014). White House Acknowledges Iraqi Airstrikes To Retake Mosul Dam Area. International Business Times, August 17th 2014. https://www.ibtimes.com/white-house-acknowledges-iraqi-airstrikes-retake-mosul-dam-area-1660806

[52] Al-Ansari, N., Adamo, N., Sissakian, V., Knutsson, S. and Laue J. (2017). Is Mosul Dam the Most Dangerous Dam in the World? Review of previous work and possible Solutions. Scientific Research Publication, Engineering 2017, 9, 801-823. https://www.diva-portal.org/smash/get/diva2:1145915/FULLTEXT01.pdf

[53] Calder, S. (2015). Andreas Lubitz: Co-pilot of Germanwings flight 9525 wanted to destroy plane in suicide and mass murder mission. The Independent, 26th March 2015. https://www.independent.co.uk/news/world/europe/germanwings-crash-suicide-and-mass-murder-by-co-pilot-10135713.html

[54] Shaw, M. (1977). Geneva Conventions 1864-1977. Encyclopedia Britannica. Accessed on 29th April 2020. https://www.britannica.com/event/Geneva-Conventions.

[55] Security Council Security Committee (2020). Information and communications technologies (ICT). United Nation. Accessed on 29th April 2020. https://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies/