Rosemary A. Burk* and Jan Kallberg*

Cyber Defense as a part of Hazard Mitigation: Comparing High Hazard Potential Dam Safety Programs in the United States and Sweden

DOI 10.1515/jhsem-2015-0047

Abstract: Cyber security tends to only address the technical aspects of the information systems. The lack of considerations for environmental long-range implications of failed cyber security planning and measures, especially in the protection of critical infrastructure and industrial control systems, have created ecological risks that are to a high degree unaddressed. This study compares dam safety arrangements in the United States and Sweden. Dam safety in the United States is highly regulated in many states, but inconsistent over the nation. In Sweden dam safety is managed by self-regulation. The study investigates the weaknesses and strengths in these regulatory and institutional arrangements from a cyber security perspective. If ecological and environmental concerns were a part of the risk evaluation and risk mitigation processes for cyber security, the hazard could be limited. Successful environmentally-linked cyber defense mitigates the risk for significant damage to domestic freshwater, aquatic and adjacent terrestrial ecosystems, and protects ecosystem function.

Keywords: Cyber defense; cyber resiliency; cyber security; dam safety; dam security; environmental security.

Disclaimer:
Rosemary Burk: The findings and conclusions in this article are those of the author(s) and do not necessarily represent the views of the U.S. Fish and Wildlife Service.
Jan Kallberg: The views expressed herein are those of the author and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, or the Department of Defense.

***Corresponding authors: Rosemary A. Burk,** U.S. Fish and Wildlife Service, Carlsbad Fish and Wildlife Office, Palm Springs, CA, USA, e-mail: rosemary.burk@gmail.com. http://orcid.org/0000-0002-9658-6768; and **Jan Kallberg,** Army Cyber Institute, 2101 New South Post Rd, Spellman Hall Room 4-33, West Point, NY 10996, USA, e-mail: jan.kallberg@usma.edu. http://orcid.org/0000-0002-0609-6985

1 Purpose of the Study

The cyber security of critical infrastructure is a top priority in the industrialized world, but tends to only address the technical intrusion in the information and control systems instead of evaluating or considering the factual impact on society, humans, urban areas, and ecosystems, if cyber security fails. This is visualized in the allocation of research funds: cyber security is focused on the technical implications and to a lesser degree environmental and societal implications. This study investigates dam safety programs and emergency preparedness in the United States and Sweden as a gage of these countries' resiliency and preparedness in the event of a successful cyberattack that would jeopardize the functionality of the dam controls. A failed cyber defense that impacts critical infrastructure could result in loss of human lives. Environmental and ecological damages can be far costlier and difficult to mitigate than the information systems and computer damages from cyberattacks.

1.1 Statement of the Problem

The lack of considerations for environmental long-range implications of failed cyber security planning and measures, especially in the protection of critical infrastructure and industrial control systems, have created ecological risks that are largely unaddressed. The study compares dam safety arrangements in the United States and Sweden. The US dam safety are in a set of states highly regulated, but inconsistent over the nation. The Swedish approach has been self-regulating dam safety. The study investigates the weaknesses and strength in these regulatory and institutional arrangements from a cyber security perspective. If ecological and environmental concerns were a part of the risk evaluation and risk mitigation processes for cyber security the hazard could be limited. Successful environmentally-linked cyber defense mitigates the risk for significant damage to domestic freshwater, aquatic and adjacent terrestrial ecosystems, and protects ecosystem function.

1.2 State Sponsored Cyberattacks

Adversarial nation states have the technical and financial capacity to launch complex attacks. In preparing a cyber defense system, it is imperative to acknowledge that potential adversaries do not subscribe to the same standards or code of ethics. To further complicate the ability to attribute a successful cyberattack is the potential for cyber weapons to be released or used by a proxy other the nation state that manufactured it. The risk posed by a hypothetical cyberattack is difficult to assess due to the number of factors, but presents a rich reward for covert

adversaries if successful. A successful cyber attack targeting high hazard dams could accomplish two key elements of a major terrorist or covert action:

1. high societal impact,
2. infliction of harm or induction of fear in the target population and societal lifelines. Societal impact would likely influence policy.

1.3 The Embedded Vulnerability

Cyberattacks have been extended beyond the Internet to target Supervisory Control and Data Acquisition (SCADA) (Stouffer et al. 2011), which are a subset of industrial control systems. SCADA systems are a part of industrial control systems that are widely used in industry, transportation, lights, and signal and the energy sector. SCADA systems, therefore are a critical component of societal technical infrastructure. These systems control the industrial processes that run our industries, chemical refineries, railroads, traffic lights and control processes in electricity generation and regulate water releases in dams by switch on or off process and electro-mechanical parts such as valves, drains, lights, electric motors, and information display.

Aside from SCADA systems developed with Internet protection features in the last decade, SCADA were not intended or designed to be connected to any other computer, let alone linked to a global information network as the Internet conduit. The failure to look beyond computer systems and not include the human as well as environmental hazards of a failed cyber defense is concerning.

2 Review of the Literature

A nation's infrastructure defense from cyberattacks is not only protecting information, network availability, or the global information grid, it is also safeguarding the lives of citizens and property and protecting ecosystems and the ecosystem services that we rely upon. Attacks on the environment and the quality of life of the citizenry directly affect the confidence the population has in the government's ability to govern (Kallberg et al. 2013). For an adversarial nation that seeks to influence a population and inject fear, cyber-created environmental damages have a high payoff, especially if the cyber operations are covert and are unlikely to be attributed. Successful environmentally-linked cyber defense mitigates the risk for significant damage to domestic freshwater, aquatic and adjacent terrestrial ecosystems, and protects ecosystem function.

The lack of considerations for environmental long-range implications of failed cyber security planning and measures, especially in the protection of critical infrastructure and industrial control systems, have created ecological risks that are unaddressed. If ecological and environmental concerns were a part of the risk evaluation and risk mitigation processes for cyber security the hazard could be limited. State-sponsored cyberattacks are likely to be perpetrated by probing IT systems well in advance of a systematic attack. These early attempts by perpetrators provide an opportunity for cyber defense by information sharing and creation of a coordinated defensive effort. The United States learned of Al-Qaeda's intentions to target dams through a series of cyberattacks in 2002 (Harnden 2002; Gellman 2002). Evidence obtained from an Al-Qaeda member's laptop computer in Afghanistan revealed logs and an internet history that offer software and programming tutorials for controlling digital switches (assumed SCADA) that control water and power facilities and during interrogations of al-Qaeda prisoners they told CIA integrators of their intent to use these switches to launch cyberattacks in America (Harnden 2002).

A two-pronged approach of a cyberattack launched simultaneously with a physical attack, for example, detonation of explosives at a dam, referred to as kinetic weapons, could lead to massive destruction. Ronald Dick, FBI's National Infrastructure Protection Center, stated in a Washington Post interview in 2002, "The event I fear most is a physical attack in conjunction with a cyberattack on the responder's 911 system or on the power grid (Harnden 2002)." In January 2013, the US Army Corps of Engineers National Inventory of Dams had a cyber breach of dam data not available to the general public. The NID contains sensitive information about dams including their vulnerabilities. Michelle Van Cleeve, a former consultant to the CIA and adviser to the Executive Agent for Homeland Security and Department of Defense was interviewed after the breach was made public and her assessment of the breach was that it was an attempt to gather information about US vulnerabilities for future cyber or military attacks (Zetter 2013). "In the wrong hands, the Army Corps of Engineers' database could be a cyberattack roadmap for a hostile state or terrorist group to disrupt power grids or target dams in this country," Van Cleeve stated (Zetter 2013).

To illustrate the evolving threat to dam security it is important to recall the British Royal Air Force (RAF) offensive Operation "Chastise" in 1943. To disrupt the industrial complex within the Ruhr Valley and munitions manufacturing and minimize Germany's ability to prolong World War II, the RAF sought to precision bomb the Mohne and Sorpe dams (Webster 2005). Plans began in 1937 to develop dam busting weaponry and refine the operational aspects of deploying bombs to achieve the maximum effectiveness in exploding high capacity concrete dams. RAF bombing of the dams resulted in breaching of the dams, widespread flooding

downstream, loss of over 1250 German lives, and disruption of the Ruhr Valley's industry (Webster 2005). British RAF lost eight planes and 54 aircrew members in the mission (Webster 2005). Although the relative success of Operation "Chastise" is still debated, key among its successes were the disruption to German transport infrastructure, and diversion of Germany's labor from Atlantic defenses to dam defenses (Webster 2005).

More difficult to quantify, but perhaps as important to the aim of the mission were: 1) the value of the attack as a propaganda material and to demonstrate Britain's ability to precision bomb and "bring the war to Germany" to their allies, 2) Britain dropped leaflets featuring their success into occupied Europe, 3) the likely psychological impact the attack had upon undermining Hitler's confidence and the move to dedicate the equivalent of a regular air-defense division to aerial defense of dams out of fear of repeat attacks (Webster 2005). A potential adversary is likely less restrained from attacking civilian dams, even if it would be against international law, because several of the potential adversaries are totalitarian regimes that have less restraints and do not subscribe to the values that created the rules of engagement in just war.

The effects of a successful cyberattack could release massive amounts of water in a short timeframe that increases the stress and likelihood for failure for dams further downstream. For example, a series of dam failures in a large watershed could result in high loss of human lives, significant property damage, widespread environmental impacts and disruption to societal infrastructure. Hydroelectric dams and reservoirs are controlled using different computer networks, either cable or wireless, and the control networks connect to the Internet. "A breach in the cyberdefenses of an electric utility company could lead all the way down to the logic controllers that instruct the electric machinery to open the floodgates" (Kallberg and Burk 2014).

Commonly, hydroelectric dams and reservoirs are built in a series along the river's length to maximize the capacity for electricity generation and take advantage of power generated by sharp declines in elevation. A cyberattack on one or more dams in the upper watershed could release water that would rapidly increase pressure on downstream dams. With rapidly diminishing storage capacity, downstream dams would be vulnerable to breach. Eventually, the attack could have a cascading effect, literally and figuratively, through the river system and result in a catastrophic flood.

The traditional cybersecurity approach is to focus on the loss of function and disruption in electricity generation – overlooking the potential environmental effect of an inland tsunami (Kallberg and Burk 2014). This is especially troublesome where the population and the industries are dense along a river, such as in Pennsylvania, Germany, and other areas with cities built around historic mills. If the

cyberattack occurred during a heavy rain when the dams were already stressed, any rapid increase in water level could trigger successive dam collapses. This could lead to high casualties and a critical loss of hydroelectric capacity. In nations seeking to maximize their hydropower capacity and deliver electricity to other countries via elaborate international electricity grids. Ensuring dam safety for these countries, such as in Sweden, becomes an issue of domestic and international importance.

3 Methodology

This paper investigates the differences in high hazard potential dams, their oversight and regulation between the United States and Sweden. The rationale for selecting United States and Sweden are the high-hazard numbers of dams and institutional differences. The method is open-source descriptive statistics, leading to a case comparison between the United States and Sweden.

The study does not have access to the actual dam protection plans, pre-event mitigation planning and efforts in place, and other classified information. Therefore, the study focused on broader indications that were openly accessible (State of California (2015).

Germany was initially studied but a significant number of the German dams are either run-of-the-river hydropower stations without a sizeable reservoir or pump storage hydropower dams. A massive release of water from a run-of-the-river dam will impact the towns and areas along the banks of the river further downstream by a slow paced flooding with no sizeable threat to human lives. Pumped storage facilities that suddenly release the water will only move the water from the higher magazine to the lower magazine, where the water masses are contained. Damage might occur in the equipment due to the sudden uncontrolled release, but threats to human lives are limited. Therefore, Germany was removed from the study.

4 Findings

The objectives of this inquiry are to;

1. outline the differences in dam characteristics and classification,
2. study institutional and emergency preparedness strengths and weakness surrounding dam safety and discuss the potential risks for harm to life or property posed by a cyber-induced dam failure,
3. discuss best practices for increasing dam safety and minimizing the risk posed by a cyberattack.

4.1 An Overview of Dams in United States

The United States Army Corps of Engineers' (USACE) National Inventory of Dams (NID) includes 87,359 dams (NID 2015). Of these, over one-third of the dams are over 50 years old (NID 2015). USACE oversees dams in excess of 50 ft. (~15 m) or 1000 storage acre-feet (~1.2 mm^3). The NID consists of dams meeting at least one of the following criteria;

1. Dams classified as high hazard. High hazard is defined as the loss of one human life is likely if the dam fails;
2. Significant hazard classification, which is defined as possible loss of human life and high likelihood of significant environmental destruction in the event of dam failure;
3. Dam height is equal to or exceeds 25 feet (~7.5 m) in height and exceeds 15 acre-feet (~18,500 m^3) in storage,
4. Dam height exceeds 6 feet (~1.8 m) in height and dam storage is equal to or exceeds 50 acre-feet (~62,000 m^3) storage (NID 2015).

Although the aim of the NID is to include all dams that meet the above criteria, limitations of funding hamper the USACE ability to gather and properly integrate dam data (NID 2015). Among challenges to maintaining the accuracy of the NID are challenges in performing consistent period assessments of dams, and identifying and resolving duplicate records (NID 2015; International Conference on Critical Information Infrastructures Security 2011).

The Federal Emergency Management Agency (FEMA) has established a dam hazard potential classification system to correspond to the magnitude of risk of a dam failure. FEMA's dam hazard classification estimates the risk of dam failure in terms of loss of human life and economic, environmental, or lifeline losses. FEMA has three hazard potential classifications: low, significant and high (Table 1) (FEMA 1998; 2007; 2013).

Table 1: FEMA's Dam Hazard Potential Classification System.

Hazard Potential Classification	Loss of Human Life	Economic, Environmental, Lifeline Losses
Low	None expected	Low and generally limited to owner
Significant	None expected	Yes
High	Probable. One or more expected	Yes (but not necessary for this classification)

Source: FEMA 2004.

The United States has a land area of 9,161,966 km^2 and is ranked third in the world in size and is over twice the size of the European Union (CIA 2015). With a population of 318,892,103 residents the United States ranks fourth in the world (CIA 2015). The number of dams by state and dam size varies considerably across the United States and largely reflects population centers and land elevation (Figure 1). High hazard dams are found in all states but are concentrated in the Appalachians, the Rocky Mountains, the Pacific Northwest and California.

Of the over 87,359 dams in the NID, 14,726 (16.6%) are classified as high hazard potential dams while the majority of dams (67.5%) in the US are categorized as having a low hazard potential (Figure 2). The data to access the factual SCADA design of high hazard dams is not accessible, so this study utilizes the presence of an Emergency Assistance Plan (EAP) as a proxy for a basic level of all-hazards preparedness.

Approximately, 60% of the high hazard potential dams in the United States have an existing EAP while 32% of significant hazard potential dams have an EAP (Figure 3).

Emergency preparedness as measured by prevalence of EAPs varies widely by state. New Jersey has only two high hazard potential dams without an EAP versus Alabama where EAPs exist for only 20% of high hazard dams (NID 2015). In addition

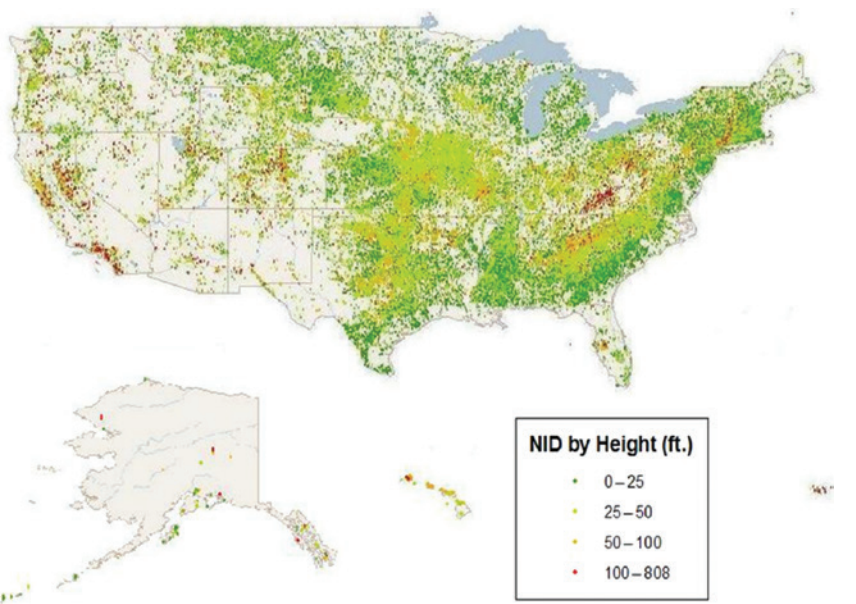

Figure 1: National Inventory of Dams (NID) Dams Classified by Height. Source: National Inventory of Dams 2015.

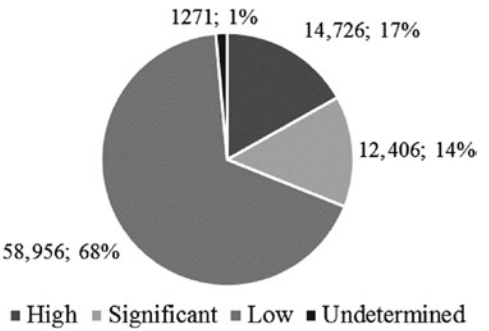

Figure 2: Dams in the United States by Hazard Potential. Source: National Inventory of Dams Database 2015.

to having a low percentage of EAPs for high hazard dams, Alabama is also the only state that has no dam safety legislation or formal dam safety program (NID 2015). To assess states' preparedness in relation to population the top four most populous states (California, Texas, New York and Florida), four least populous states (Alaska, North Dakota, Vermont, and Wyoming), and four states selected using a random number generator (Random 2014) were studied. Oregon, Arizona, Georgia and New Mexico were randomly selected for comparison (Figures 4 and 5).

Populous states with the highest relative percentage of completed EAPs are New York, Texas, California and Florida, respectively. However, a ranking of populous states by highest number of high hazard potential dams lacking EAPs reveals a different order: Texas (354), Florida (49), New York (19) and California (12). California stands out among the most populous states in its high number of high hazard dams that do not require an EAP. The randomly selected states of Oregon, Arizona, Georgia and New Mexico reflect states of varying geography,

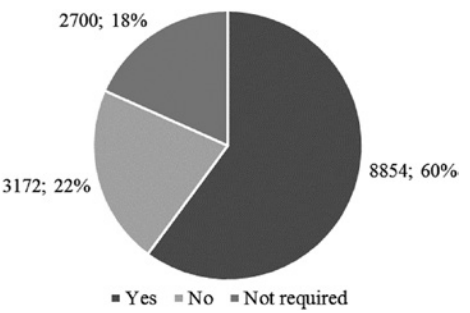

Figure 3: Number of High Hazard Potential Dams with an existing Emergency Action Plan (EAP). Source: National Inventory of Dams Database 2015.

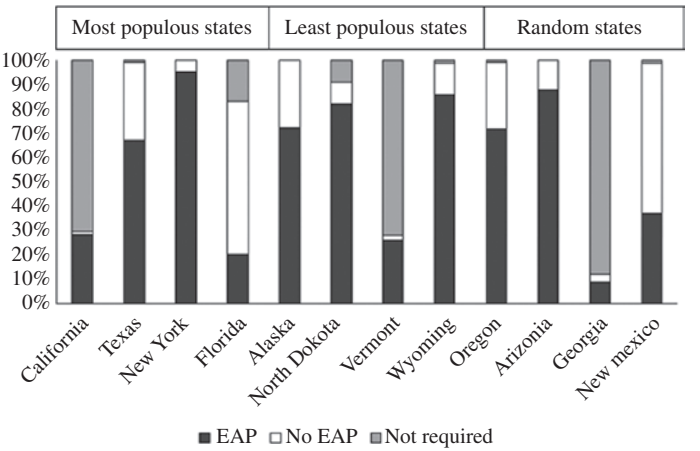

Figure 4: Relative Percentage of High Hazard Potential Dams with and without an EAP. Data source: National Inventory of Dams 2015.

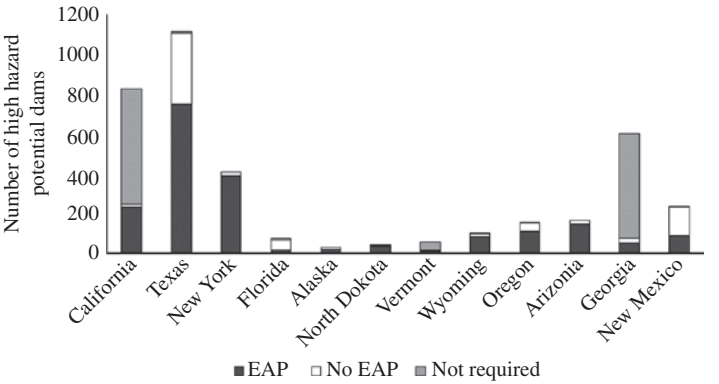

Figure 5: Number of High Hazard Potential Dams with and without an EAP. Data source: National Inventory of Dams 2015.

dam types, population densities and economies. They are located on the west coast, southwest, and south-central United States. Oregon has roughly one-fourth of the high hazards dams compared to neighboring California. Seventy percent of the high hazard dams in Oregon have an EAP, compared to less than 30% of California's high hazard dams; however, California does not require EAPs for over 2/3 of their high hazard dams (Figure 4). Oregon has a slightly higher number of high hazard dams without EAPs than does California, but lacks the high number of high hazard dams that do not require an EAP. The difference in EAP preparedness between Arizona and New Mexico may reveal a difference in these state's

resources and population densities. Among US states, Arizona ranks 33rd (right before Arkansas at 34th) and New Mexico ranks 45th for population densities (US Census Bureau 2014). Arizona's population density is 58.2 persons/mi^2 (~33 persons per km^2) compared to New Mexico's 17.2 persons/mi^2 (~7 persons per km^2) (US Census Bureau 2014). From this small sample of 12 states, it is evident that the extent of emergency preparedness as indicated by number of EAPs for high hazard potential dams, varies widely across the United States. Furthermore, not all states have a dam safety program. Dam owners that operate a high hazard potential dam are required to complete an EAP. However, the national average of high hazard potential dams with EAPs is 69% (NID 2015).

Key strengths related to dam safety and lowered cyber-attack risk in the United States are:

1. regulatory oversight and periodic inspection of high hazard dams by USACE engineers;
2. FEMA's leadership in adopting an all-hazards approach in emergency management,
3. a consistent hazard classification is used for all dams in the United States,
4. hazard assessment to human lives and property are considered alongside environmental hazards at the federal level.

Potential weaknesses in dam safety programs and emergency preparedness include:

1. there are over 14,500 high hazard dams in the United States,
2. not all states require dam owners to prepare, test for and update EAPs,
3. the vast majority of dams are privately owned making a consistent application of dam safety regulations and addressing dam weaknesses resource intensive,
4. dam safety programs and emergency preparedness planning (EAPs) for high hazard dams varies greatly by state making a federally equitable evaluation of dam safety priorities and hazards challenging,
5. inability for dam operators to share intelligence related to potential attacks, cyber or physical, and learn from cyberattack probing attempts,
6. failure of some of the nation's high hazard dams would result in flooding downstream of highly populated cities for example, Phoenix, AZ, Jersey City, NJ, and Los Angeles, CA.

Findings from FEMA's (2007) report Emergency Action Planning for State-Regulated High Hazard Potential Dams recommendations for increasing dam safety, included:

1. improved coordination and communication between private dam owners and federal and state agencies,
2. improved communication of dam failures,

3. improvements to EAP documentation,
4. mapping of non-federal high hazard dams,
5. not all states require EAP's for high-hazard potential dams,
6. limited funding for Emergency Action Planning for dams undermines the mission of protection of life and property (FEMA 2007).

4.2 An Overview of Dams in Sweden

Sweden is a county with a landmass of 450,295 km^2 an area slightly larger than the state of California and is bordered on the east by Norway and the west by Finland (CIA 2015). The population of Sweden is estimated to be 9,723,809 (CIA 2015). In contrast to semi-arid California with over 38 million people, Sweden is a water-rich country with low population densities and little reliance upon irrigated agriculture.

There are approximately 10,000 dams in Sweden. Roughly 27% of dams in Sweden are classified in the highest hazard classification, 1A (Svenska Kraftnät 2010) (Figure 6). Most of these high hazards dams are owned by major utilities and found along powerful, regulated hydropower rivers (Figure 7 and Table 2). Failure of these dams could cause loss of human lives, destruction of property, disruption in communication and transportation, and serious economic or environmental damage. It is estimated that a dam failure among any of the 20–30 large high hazard dams, including Sourva dam that has twice the storage as Hoover dam, would result in grave consequences (Svenska Kraftnät 2010). Sweden relies heavily on hydropower for generation of electricity. Currently, hydropower accounts for roughly half of the overall electricity production in the country, which is generated by 200 large scale hydropower dams (>10 MW) and 1600 smaller hydropower dams (Vattenportalen 2007). Most of the hydropower

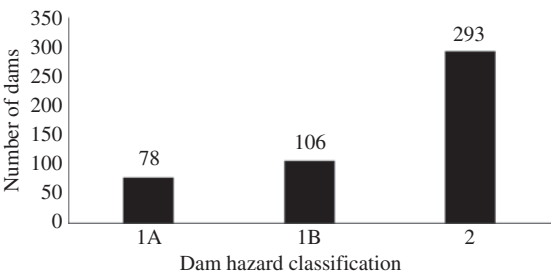

Figure 6: Hazard Classification of Sweden's Dams using the RIDAS System. Data source: Svenska Kraftnät (2010).

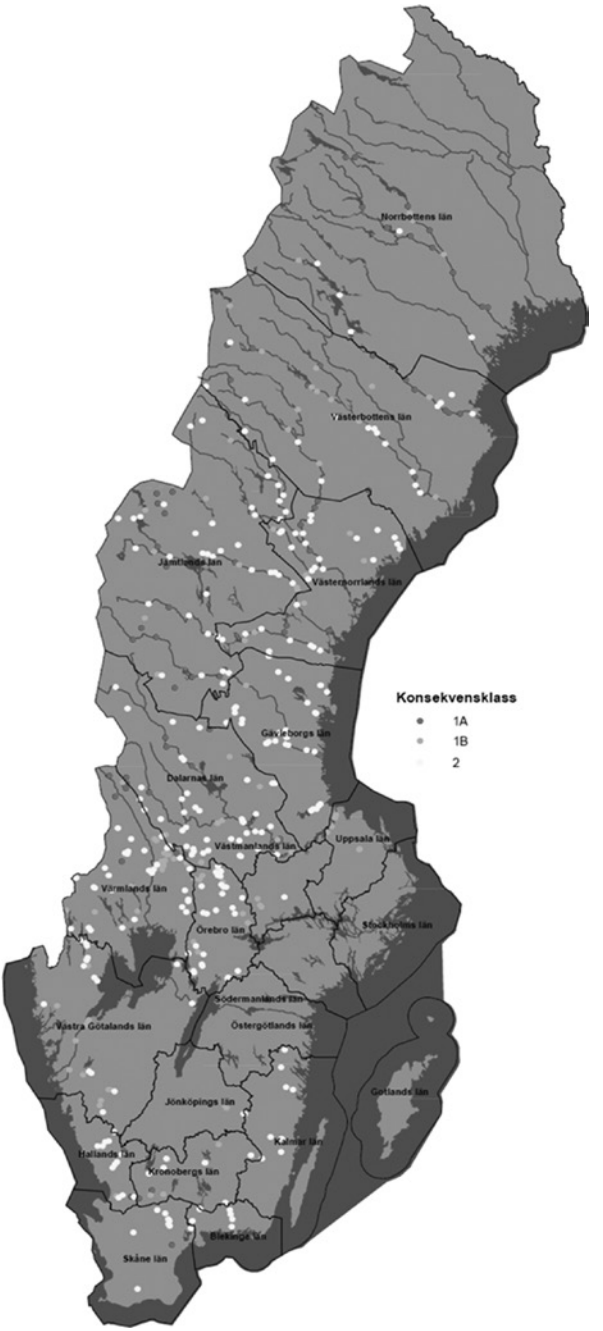

Figure 7: Hazard Classification of Dams in Sweden. Map Source: Svenska Kraftnät (2010).

Table 2: Number of Class 1A Dams in Sweden and their Distribution in Counties of the Largest Dam Owners (Svenska Kraftnät 2010).

Dam owner	Class 1A Consequence Dams	Number of Counties with Dams
Hydropower		
Vattenfall	21	5
Fortum	21	4
The Östersund water regulation enterprises at the rivers: Dalälven, Ljusnan, Ljungan, Indalsälven, Ångermanälven, and Umeälven (all managed by same organization)	13	2
Statkraft	9	5
Skellefteå Kraft	3	2
E. ON	4	2
Boliden Mineral	N/A	N/A

dams are along the length of the river and form a cascades and impounded reaches. Failure of these dams could create a chain of dam failures downstream along the entire stretch of the river to coast and "bring about serious disturbances in activities vital to society" (Svenska Kraftnät 2010).

There are eight separate dam owners with dams classified as 1A and these same dam owners also own and operate the majority of dams of consequence class 1B and 2 (Svenska Kraftnät 2010) (Table 2).

Dam safety regulation is outlined in a patchwork of regulations, the most important of these being the Civil Protection Act and Swedish Environmental Code (Svenska Kraftnät 2010). Regulations are divided by different agencies with no operative experience that act only as regulatory bodies. Dam safety legal regulations require dam safety to meet a "high international standard," but does not specify a model (Svenska Kraftnät 2010).

Svenska Kraftnät is the government authority responsible for the security of the electric grid and electricity preparedness as well as coordination of Sweden's dam safety (Svenska Kraftnät 2014). Established in 1992, it operates as a public utility that generates revenues through assessing fees to electricity producers for use of the national grid.

Dam safety is largely left to the dam owner's and with no centralized and clear dam safety regulations, the major utilities have little direction for safeguarding lives, property and environment and are solely liable for damages caused by the dam failure (Svenska Kraftnät 2010).

Unlike in the United States with a high amount of federal oversight and emergency preparedness for dams classified as high hazard, the authority and

responsibility for dam safety in Sweden resides largely within counties. The county administrative board, as specified by the Environmental Code, provides operational supervision of water operations including dam safety (Svenska Kraftnät 2010). Since all private owners of 1A Consequence dams have dams distributed across multiple counties (Table 2), this poses a logistical challenge for dam safety management from the owner's perspective. While local control may have benefits one large drawback would be the lack of a comprehensive evaluation of dam safety practices, best practices, and risk evaluation. County administrative boards are also charged with providing for emergency preparedness planning within their jurisdictions and are expected to be able to assume the duty of local rescue in the event of a dam failure (Svenska Kraftnät 2010).

Environmental concerns and risks are an issue for county and local governments meanwhile other issues such as human hazards are evaluated at the national level.

Due to the remote location of most of the dams of consequence class 1A and 1B, hydroelectric dams are managed with a high level of centralization to reduce labor cost. Access to good wireless reception is available even in remote locations making centralization and remote control of dams possible. A control center can control up to 30–40 large and mid-size hydro-electrical dams and numerous water level regulating dams. The midsize dams and smaller dams are mainly controlled by wireless data link. One control center controls 18% of Sweden's hydropower (Svenska Kraftnät 2009).

4.2.1 Swedish Dam Safety Shortfalls

1. Dam safety and emergency preparedness does not follow an all hazards approach – instead considerations of dam safety are limited to supra-seasonal precipitation and technical standings.
2. There are a limited number of control centers with no ability to manually override the systems within hours. Sometimes, competent key personnel are located 200–300 km away.
3. There is a high reliance on wireless controls throughout most of Sweden's high hazard dams.
4. A few large utilities dominate the hydropower market and they have gained the trust of government which leads to self-regulation creating an inconsistent dam emergency preparedness across the country.
5. Heavy reliance on hydropower by Sweden and in the future other countries as Sweden is in the process of extending their grid to Germany and other neighboring countries, puts a heavy emphasis on power generation reliability

and maximum production. Towards this end, international interest in the reliability and safety of Sweden's dams should provide an impetus to address shortfalls in their dam safety programs and move towards an integrated all-hazards model similar to the United States.

5 Conclusions and Recommendations

The individual threat of a successful cyberattack to a dam should not be overstated, but planned for. The threat posed by a cyberattack is inherently difficult to quantify and not all dams are vulnerable nor pose a hazard to surrounding populations if a failure occurred. However, the threat is real and dams are an attractive target for adversaries that seek to disrupt and destabilize society.

The payoff of a potential terroristic cyberattack would be very high as it erodes trust the targeted government's population has in their government's ability to govern and provide security. One major successful attack would influence a national confidence in the government's ability to provide a safe living environment.

Two-pronged kinetic and cyberattacks to dams when dams or populations downstream are at their most vulnerable could prove especially deadly. So far Sweden has not experienced a dam failure of devastating consequences and loss of human lives, but the United States has, notably in flooding caused by levee failure that caused exceptional flooding in New Orleans after Hurricane Katrina and loss of over 1400 human lives. Similarly, a two-pronged attack to dams would be most deadly and destructive if conducted while dams are at their capacity due to above average precipitation or during periods of rapid snowpack melting. The impact of these attacks is based on the absence of planning for cyber resiliency.

5.1 Policy

A policy concern identified in this study is the degree of freedom states in the United States have to determine their standards for dam safety. If there are no regulatory interest to regulate and standardize dam safety in general, the cyber security aspects will then be a matter of the dam owner's own interest and if it is seen as a problem on a local level. Cyber risks are abstract, until they become attacks, and require specific domain knowledge that could be unevenly distributed in the industry. In the absence of rules and regulation it is likely that cyber risks are addressed in a fraction of the conducted planning and mitigation processes.

The study also raises questions about the balance between regulatory requirements for cyber security for dams and the reliance on self-regulation within the industry, which in most societies is a matter of ideological outlook and beyond the scope of this study.

5.2 Practice

A practice that this study suggests is general and applies to any country with high hazard dams. Even if dam control is automated and remotely controlled through wireless communication, there is a need to ensure that these instructions can be manually overridden, and the dam owner can maintain control over the dam activity even if cyberattacked. The dependency on wireless and remote control is a growing vulnerability as dam control is becoming more centralized and based on digital communications for commands to the dams and related facilities.

5.3 Future Research

Cyber security research within the realm of computer science and engineering is generally more focused on defending the information systems without addressing the potential societal and environmental consequences of a failed cyber defense. Emergency management as a discipline is academically focused on assessing the consequences, mitigating risks, and handling potential outfalls. Dam-related cyber security is an opportunity for multi-disciplinary research that merges computer science, engineering, emergency management, and natural resources management.

References

Central Intelligence Agency (CIA) (2015) The World Fact Book. Available at: https://www.cia.gov/library/publications/the-world-factbook/geos/sw.html (accessed January 16).

Federal Emergency Management Agency (FEMA) (1998) *Federal Guidelines for Dam Safety: Hazard Potential Classification System for Dams*. Available at: http://www.fema.gov/media-library-data/20130726-1516-20490-7951/fema-333.pdf.

Federal Emergency Management Agency (FEMA) (2007) *Emergency Action Planning for State Regulated High-Hazard Potential Dams: Findings, Recommendation, and Strategies.* FEMA 608. Retrieved from http://www.fema.gov/media-library-data/20130726-1624-20490-6709/fema608.pdf.

Federal Emergency Management Agency (FEMA) (2013) *Federal Guidelines for Dam Safety*. FEMA 64. Available at: http://www.fema.gov/media-library-data/5b20db599c212f77fd5e85d256f471a3/EAP002BFederal002BGuidelines_FEMA002BP-64.pdf.

Gellman, B. (2002) Cyberattacks by Al Qaeda Feared. *The Washington Post*. June 27. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html.

Harnden, T. (2002) Al-Qa'eda plans Cyber attacks on dams. *The Telegraph*. June 28. Available at: http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1398683/Al-Qaeda-plans-cyber-attacks-on-dams.html.

International Conference on Critical Information Infrastructures Security (2011) September 2011 National Inventory of Dams. Available at: http://cordis.europa.eu/event/rcn/33342_en.html.

Kallberg, J. and R. Burk (2014) "Failed Cyberdefense: The Environmental Consequences of Hostile Acts," Military Review, 92:22–25.

Kallberg, J., B. Thuraisingham and E. Lakomaa (2013) "Societal Cyberwar Theory Applied: The Disruptive Power of State Actor Aggression for Public Sector Information Security." In: Proceedings of the 2013 Intelligence and Security Informatics Conference (EISIC), European, Piscataway: IEEE Press, pp. 212–215.

National Inventory of Dams (NID) (2015) National Inventory of Dams website maintained by U.S. Army Corps of Engineers. Available at: http://geo.usace.army.mil/pgis/f003Fp003D397:5:0::NO (accessed January 10).

Random.org (2014) Available at: http://www.random.org (accessed December 4).

State of California (2015) California Office of Emergency Services. Dam Safety Action. Available at: http://www.damsafetyaction.org/CA/ (accessed January 16).

Stouffer, K., J. Falco and K. Scarfone (2011) "Guide to Industrial Control Systems (ICS) security," NIST Special Publication, 800–882.

Svenska Kraftnät (2009) *Peer-review of Swedish High Consequence Dams: Test of a model for "special examination" of dam safety. A compilation of facts and experiences from 5 reviews performed in 2006–2008*. Available at: http://www.svk.se/Global/09_About_Us/Pdf/Peer-Review-Swedish-High-Consequence-Dams.pdf.

Svenska Kraftnät (2010) Review of the Swedish System for Dam Safety: A Report to the Government. Available at: http://www.svk.se/Global/09_About_Us/Pdf/Review-Dam-Safety-12-aug-2011.pdf.

Svenska Kraftnät (2014) About us. Available at: http://www.svk.se/Start/English/About-us/Our-Activities/ (accessed December 4).

United States Census Bureau (2014) Population Estimates: State Totals. Available at: http://www.census.gov/popest/data/state/totals/2013/ (accessed December 4).

Vattenportalen (2007) Vattenkraft och stora dammar [Hydro power and major dams]. Available at: http://www.vattenportalen.se/fov_problem_vattenkraft.htm.

Webster, T.M. (2005) "The Dam Busters Raid: Success or Sideshow?" Air Power History Summer 34:13–25.

Zetter, K. (2013) Hacker breached U.S. Army Database Containing Sensitive Information on Dams. Wired.com. Available at: http://www.wired.com/2013/05/hacker-breached-dam-database/.