IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

Policy Brief

The Cyber Terrorism Landscape for Dams in Pakistan

Maham Naweed
Hajra Hashmi

March 2025

Chair International Law

Executive Summary

Dams are an integral part of the water infrastructure in Pakistan. The construction of major dams was aimed at regulating and supporting the flow of water in irrigation systems to sustain the country's agricultural sector. These dams are primarily managed to meet the nation's irrigation needs, with the generation of low-cost hydroelectricity serving as an additional benefit. They also are vital tools in preventing flooding in many areas of the country.

International law emphasizes the need for the responsible management and protection of water resources, particularly when it comes to water infrastructure such as dams. In this context, the focus shifts to domestic regulations, ensuring that water resources are used sustainably and that their management does not harm the environment or deplete resources for future generations. International law encourages states to protect water bodies by adhering to principles of environmental sustainability, with particular attention to the ecological impacts of dam construction and operation. While the immediate concern may not involve neighboring countries, international conventions, such as the Convention on Biological Diversity or the Ramsar Convention on Wetlands, may still apply if the water resources have global significance, such as supporting biodiversity or regulating climate patterns. Ultimately, the responsibility to protect these resources remains with the nation, which must ensure that its use of water resources aligns with global standards for environmental protection and sustainability.

Dams in Pakistan are operated and maintained by the Water and Power Development Authority (WAPDA) and provincial governments. They control when water is released or contained, according to the needs of the environment and region. In order to do so, specific technological systems are used; the monitoring and operation of dams depends on these technologies.

Due to their integral role in the preservation of natural resources, dams are prime targets for terrorist attacks. Along with the 'traditional' threat to the physicality of the structures themselves, a new, potentially more destructive threat has emerged: that of a cyber takeover. Non state actors have started hacking into the cyber systems that control dams in some places in the world, which is a major concern that Pakistan needs to anticipate, as our economy is largely dependent on water. A cyber takeover of a dam also poses an extreme threat to the people and infrastructure surrounding the dam as strategic use of the water by cyber terrorists could cause large scale flooding in the area.

Policy Recommendations

- Cyber audits need to be made compulsory for all the major and minor dams of Pakistan that use software systems to control the workings of the dams. A cyber audit is an evaluation process designed to assess the cybersecurity measures, policies, practices, and controls of an organization to identify vulnerabilities, risks, and compliance with relevant standards or regulations. The goal is to ensure that an organization's digital infrastructure, including networks, systems, and data, is adequately protected against potential cyber threats and breaches. Conducting thorough cyber audits once a year would ensure better cyber security for the dams of the country.
- Specific national cyber security policies, aimed towards the protection of national resources rather than all-encompassing ones, need to be drawn up. This will strengthen the security measures in place for dams and better protect them from potential breaks in defence mechanisms.
- Software systems for dams must be regularly fortified. Firewalls and Intrusion Detection Systems need to be installed and updated in order detect and block unauthorized access attempts. Measures such as the isolation of critical control systems (e.g., SCADA systems) from general networks should be taken to limit exposure to cyberattacks.
- Specialized cybersecurity teams capable of responding to cyberattacks on critical infrastructure must be established. Trained response experts must be allocated to each dam in order to have constant security in place.

History Of Water Management in Pakistan

After gaining independence, Pakistan inherited a well-developed irrigation system from British India, based on the Indus River system. Major canals were developed during the British colonial period such as the Chashma-Jhelum Link Canal which were crucial for irrigation in the agricultural economy of the region. However, as Pakistan became independent in 1947, the country was tasked with managing the distribution of water resources, especially in the face of its significantly growing population and agricultural demands.

Pakistan's river system is largely based on the Indus river and its tributaries, namely the Jhelum, Ravi and Chenab. Since these waters either originate in, or are linked to other Indus tributaries in, India, it was crucial to come to an agreement over their use. The Indus Water Treaty was signed between Pakistan and India in 1960 to help manage water resources.[1] Under the treaty, Pakistan received control of the three eastern rivers; Jhelum, Chenab, and Ravi, while India gained control of the three western rivers, namely the Sutlej, Beas, and Bias. This agreement was seen as a way to avoid conflict over shared water resources and to promote peaceful relations.

In the 1960s and 1970s, Pakistan undertook significant efforts to develop its water infrastructure. The Tarbela Dam was constructed, which is one of the world's largest earth-filled dams. The dam, located on the Indus River, plays a critical role in irrigation and electricity generation. The Mangla Dam was built on the Jhelum River which provided substantial irrigation and power generation. These two dams are referred to as the backbone of Pakistan's water management system.

In the early 2000s, the Water and Power Development Authority (WAPDA), responsible for the development of hydropower projects and water infrastructure, faced increasing challenges in maintaining existing infrastructure and addressing the needs of a growing population. Therefore, Pakistan began developing more comprehensive water management policies, including the National Water Policy of 2002, aimed at addressing water scarcity and inefficiencies in water use.[2]

[1] Indus Water Treaty.
[2] National Water Policy 2002.

Current Dams and Their Administration

WAPDA is the central authority responsible for the planning, development, and maintenance of dams in Pakistan. It oversees the construction and operation of major dams, ensuring they meet the country's water storage, irrigation, and power generation needs. It also coordinates with provincial governments and other stakeholders to manage water resources effectively and to address regional requirements.

In recent years, the military has also become increasingly involved in economic projects, including large infrastructure initiatives like canal construction and dam projects. The Special Investment Facilitation Council (SIFC), co-led by the army chief, oversees various initiatives, which has led to discussions about the military's progressive role in economic development. Overall, the administration of dams in Pakistan involves a combination of federal agencies, provincial authorities, and, in some cases, military involvement, all working together to manage the country's water resources and infrastructure projects.

The administration of dams is decentralized. Despite all of them falling broadly under the authority of the groups mentioned above, each dam has its own team and dedicated software systems solely responsible for that dam in question. Information is passed between teams, such as statistics related to water quantity, weather conditions, etc, but the actual workings of each dam are separate and unique. This means that if for some reason one of the dams is compromised in any way, the rest will remain unaffected. Access to the control rooms for the dams is extremely restricted, so only a select few people know the actual internal workings of the project they are assigned to. Decentralization serves as a very effective method of protection and it has served Pakistan’s water systems well so far. However, the newly emerged threat of cyber attacks on dams requires more stringent policies.

Terrorism and Dams

Water resources have long been a target of parties to conflicts. Compromising the water resources of a country is a huge blow to the wellbeing of its people as well as to its economic capabilities. Throughout history, water supplies have been used as turning points in wars. In 1000 BC, Chinese warriors used arsenic to contaminate their enemies' water supplies.[3] The Roman army used water, both as an offensive and defensive weapon, including diversion of

[3] Frith, J. Arsenic-the “poison of kings” and the “saviour of syphilis”. *J. Mil. Veterans Health* 2013, *21*, 11–17.

water, thus preventing besieged populations from its most vital resource.[4] Using the water of an area against its own people is an ancient tactic of war.

However, in more recent times, non-state actors have begun to use water and dams to their advantage. This adds an entirely new dimension to the problem, as conflicts with terror groups are much more difficult to regulate or classify under international legal regimes. One of the most prominent cases in which a terrorist group used water sources to its advantage is that of ISIS' attack on the Iraqi town of Snune. After taking control of the area, they poisoned or sabotaged every well they could find, making it uninhabitable.[5]

Taking it a step further, terror groups have also started taking over water resources such as dams for long-term control. In 2013, ISIS captured the Tabqa Dam, using it as a headquarters, prison, and training site. They also employed it as a control center for attacks against Western targets.[6] In September 2014, ISIS took control of the Tishrin Dam, a crucial infrastructure on the Euphrates River. It was captured by the Syrian Democratic Forces (SDF) in December 2015, restoring control to Kurdish-led forces.[7] In December 2024, the Turkish-backed Syrian National Army (SNA) launched an offensive against Kurdish forces near the Tishrin Dam, aiming to gain control over the area. This conflict has led to civilian casualties and heightened tensions in the region.

CYBER TERRORISM AND DAMS

The connection between cyber terrorism and dams is a very new phenomena. As illustrated in the section above, water is a prime target for non-state groups looking to gain footing in an area. Due to the use of software in the administration of dams, the new threat of cyber attacks combined with the crucial role that dams play in water management for all countries, has led to the very real threat of cyber terrorism to water infrastructure.

[4] Angelakis, Valipour, et al, 'Water Conflicts: From Ancient to Modern Times and in the Future' (2021) https://www.proquest.com/docview/2562195947?sourcetype=Scholarly%20Journals accessed 20 February 2025.
[5] Peter Schwartzstein , 'The History of Well Poisoning' (2019) https://www.smithsonianmag.com/history/history-well-poisoning-180971471/ accessed 20 February 2025.
[6] Cheryl Pellerin, 'Local Forces Launch Daring Assault Behind Enemy Lines in Syria' (22 March 2017) https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/1127560/local-forces-launch-daring-assault-behind-enemy-lines-in-syria/ accessed 20 February 2025.
[7] Dursun Yıldız, 'Who Controls Syria's Dams on the Euphrates River: An Overview' (20 December 2024) https://www.hidropolitikakademi.org/en/article/31076/who-controls-syrias-dams-on-the-euphrates-river-an-overview accessed 20 February 2025.

In 2013, Iranian hackers infiltrated the Bowman Avenue Dam in Rye Brook, New York, marking a significant cyber intrusion into U.S. critical infrastructure. The attack was part of a broader campaign by the Islamic Revolutionary Guard Corps (IRGC) targeting various U.S. entities. The hackers accessed the dam's Supervisory Control and Data Acquisition (SCADA) system via a cellular modem, enabling them to monitor operational data such as water levels and sluice gate status. Although the hackers gained unauthorized access, they did not manipulate the dam's operations. At the time, the sluice gate was manually disconnected for maintenance, preventing potential remote control.[8]

Although no damage was caused by this specific attack, it is a very alarming incident that must be taken extremely seriously. If terrorist groups are capable of remotely taking control of crucial infrastructure such as dams, that means they could potentially wreak havoc on a country's essential services sectors from a distance. It opens the path for entire governments to potentially be undermined. Therefore, it needs to be addressed in a preventive manner.

APPLICABILITY TO PAKISTAN

While there have been no widely reported cyberterrorist attacks on dams in Pakistan, the existing vulnerabilities and the critical nature of these infrastructures make them potential targets. It is imperative for Pakistan to strengthen its cybersecurity measures, particularly for critical infrastructure like dams, to mitigate the risks associated with cyberterrorism.

Due to its history with terrorism and terror groups operating across the South Asian region, the country needs to practice preventive measures in order to avoid compromised dams and water sources. Water and wastewater systems are among the most vulnerable to cyberattacks, which can disrupt operations and pose safety risks. Given the critical role of dams in water management, any compromise could have severe consequences.

Pakistan has recognized the importance of cybersecurity and developed the National Cybersecurity Policy 2021 to address emerging threats.[9] This policy aims to enhance the security of digital systems and protect citizens from cyber risks. While it is a great step in the right direction, the threat of cyber terrorism is evolving at such a quick pace that specified

[8] G Cohen, 'Throwback Attack: How The Bowman Avenue Dam Became The Target Of Iranian Hackers' (12 August 2021) https://www.controleng.com/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/?utm_source=chatgpt.com accessed 20 February 2025.
[9] National Cybersecurity Policy 2021.

policies aimed to protect national infrastructures need to be developed in order to avoid large scale damage to resources such as dams.

RECOMMENDATIONS

- Cyber audits need to be made compulsory for all the major and minor dams of Pakistan that use software systems to control the workings of the dams. A cyber audit is an evaluation process designed to assess the cybersecurity measures, policies, practices, and controls of an organization to identify vulnerabilities, risks, and compliance with relevant standards or regulations. The goal is to ensure that an organization's digital infrastructure, including networks, systems, and data, is adequately protected against potential cyber threats and breaches. Conducting thorough cyber audits once a year would ensure better cyber security for the dams of the country.
- Specific national cyber security policies, aimed towards the protection of national resources rather than all-encompassing ones, need to be drawn up. This will strengthen the security measures in place for dams and better protect them from potential breaks in defence mechanisms.
- Software systems for dams must be regularly fortified. Firewalls and Intrusion Detection Systems need to be installed and updated in order detect and block unauthorized access attempts. Measures such as the isolation of critical control systems (e.g., SCADA systems) from general networks should be taken to limit exposure to cyberattacks.
- Specialized cybersecurity teams capable of responding to cyberattacks on critical infrastructure must be established. Trained response experts must be allocated to each dam in order to have constant security in place.

Action Matrix				
Options for Pakistan				
Option	**Pathways to Solution**	**Implementation of Solution**	**Actors Responsible**	**Implementation Timelines**
Mandate annual cyber audits for all dams	Create a viable plan for yearly cyber audits of all dams in Pakistan.	Commission or employ cyber security experts to carry out this audit on a yearly basis.	Ministry of Information, Technology and Telecommunications. Ministry of Water Resources. Water and Power Development Authority (WAPDA).	4-6 months for the training and background check of experts.
Establish specialized national policies	Establish policies and regulations targeted specifically towards the cyber security of national	Ensure the implementation of these policies at all major and minor dams across the country.	Ministry of Information, Technology and Telecommunications.	1-2 years for establishment and framework creation.

	infrastructure, such as dams.		Ministry of Water Resources. Water and Power Development Authority (WAPDA).	
Allocate cyber security specialists to each dam	Research and hire cyber security specialists from the private sector.	Place one or multiple of these experts, as per the needs of the dam project in question, at each dam across the country.	Ministry of Information, Technology and Telecommunications. Ministry of Water Resources. Water and Power Development Authority (WAPDA). Private actors.	6-8 months for scouting and hiring. Additional 2-3 months for training and posting.