water

MDPI

Review

A Systemic Review of the Cybersecurity Challenges in Australian Water Infrastructure Management

Abubakar Bello [1], Sayka Jahan [2], Farnaz Farid [1,*] and Farhad Ahamed [3]

[1] School of Social Sciences, Western Sydney University, Sydney, NSW 2751, Australia
[2] Department of Earth and Environmental Sciences, Macquarie University, Sydney, NSW 2109, Australia
[3] Kent Institute Australia, Sydney, NSW 2000, Australia
* Correspondence: farnaz.farid@westernsydney.edu.au

Abstract: Cybersecurity risks have become obstinate problems for critical water infrastructure management in Australia and worldwide. Water management in Australia involves a vast complex of smart technical control systems interconnected with several networks, making the infrastructure susceptible to cyber-attacks. Therefore, ensuring the use of security mechanisms in the control system modules and communication networks for sensors and actuators is vital. The statistics show that Australia is facing frequent cyber-attacks, most of which are either undetected or overlooked or require immediate response. To address these cyber risks, Australia has changed from a country with negligible recognition of attacks on critical infrastructure to a country with improved capability to manage cyber warfare. However, little attention is paid to reducing the risk of attacks to the critical water infrastructure. This study aims to evaluate Australia's current cybersecurity attack landscape and the implemented controls for water infrastructure using a systematic literature review (SLR). This study also compares Australia in the context of global developments and proposes future research directions. The synthesis of the evidence from 271 studies in this review indicates the importance of managing security vulnerabilities and threats in SCADA water control systems, including the need to upgrade the contemporary water security architecture to mitigate emerging risks. Moreover, human resource development with a specific focus on security awareness and training for SCADA employees is found to be lacking, which will be essential for alleviating cyber threats to the water infrastructure in Australia.

Keywords: smart water system; cyber security; water infrastructure; cyber-physical systems; Internet of Things (IoT)

check for updates

Citation: Bello, A.; Jahan, S.; Farid, F.; Ahamed, F. A Systemic Review of the Cybersecurity Challenges in Australian Water Infrastructure Management. *Water* **2023**, *15*, 168. https://doi.org/10.3390/w15010168

Academic Editor: Marco Franchini

Received: 23 November 2022
Revised: 28 December 2022
Accepted: 29 December 2022
Published: 31 December 2022

1. Introduction

A smart water infrastructure system is an integral part of any metropolitan city. It comprises an integrated network of sensors and actuators connected to programmable logic controllers (PLCs). It is managed by a supervisory distributed control system (DCS) and data acquisition (SCADA) system [1,2]. The benefits of a smart water infrastructure system include the ability for accurate water consumption measurements, safe and reliable water supply, wastewater treatment, flood prevention and monitoring, and water wastage control [3–9]. Regardless of the many advantages of incorporating modern technologies into water infrastructure systems, there are many security risks and challenges in preventing supply disruptions, water theft, water poisoning, and water wastage. Connecting the water infrastructure's physical components with the cyberspace exposes these systems to the broad domain of cyber-grounded threats [10,11].

Water is a fundamental resource that has no possible substitute. Its usage as a diplomatic tool or military target has a long history [12]. From a national security perspective, water infrastructure plays a vital role in a nation's sustainable development, making it highly susceptible to cyber-attacks. Formerly, cyber criminals are either individual actors or small hacker groups. However, various state-run organisations can carry out targeted attacks using sophisticated malware and zero-day exploits.

Previously, the security of water systems was mainly maintained through their remoteness and by restricting access to the control components. However, with the advent of the Internet of Things (IoT), like other critical infrastructure services, water infrastructure systems have progressively adopted intelligent systems technologies. Therefore, they are now susceptible to cyber–physical attacks (CPA) that can target the SCADA module (system processes monitoring), the PLCs that run the substantial elements of the system, or the remote communication network, among the other components of the cyber–physical system (CPS). Cyber-attacks could be launched remotely by employing command and control techniques to interrupt the system's performance and provide access to illegitimate parties to critical and confidential information. Moreover, in more severe cases, such attacks can even cause physical impairment to the system's structure. Furthermore, such attacks can hamper the water quality by changing the treatment systems or suppressing contamination warnings by affecting water quality sensors.

The last decade has witnessed a noticeable number of severe cybersecurity cases connected to water infrastructure systems. The US Department of Homeland Security (DHS) considers the water and wastewater infrastructure system (WWIS) as one of the primary victims of cyber-attacks among the 16 lifeline infrastructure sectors [13]. They declared that safeguarding the WWIS against cybersecurity threats is now a national priority [14]. According to ICS-CERT, in 2015, about 25 cybersecurity incidents were reported by various water utilities, making WWIS the third most targeted sector [15]. However, with the advancement of modern security technology, one may assume that the cybersecurity risks to the WWIS are low and most of the water infrastructure systems are reliable and secure. However, many cybersecurity incidents in these systems either go undetected or unreported. In some cases, they are not disclosed to safeguard the customer's trust, the victim's reputation, and revenue [16–19].

Australia is also facing a dramatic increase in the number of cyber-attacks. The statistics show that between 2011 and 2012, Australia experienced about 438 cyber incidents requiring an immediate and profound response by the Cyber Security Operation Centres and the Australian Federal Government [20]. In Australia, modern water infrastructure systems are operated by industrial control systems (ICSs) consisting of DCS, PLC, and SCADA systems. However, the SCADA systems in Australia are different and very complex due to the remoteness of many of the utility plants and field stations and the vastness of the country [21]. Hence, the SCADA systems in Australia are more susceptible to cyber threats. A well-cited example is the SCADA security incident at Maroochy Water Services in Queensland, Australia, in 2000. This was the first global example (declared publicly) of a successful hacking case against a critical SCADA infrastructure system [22], resulting in an urgent need to ensure a secure water distribution system that controls the water quality and the central water infrastructure system [23,24].

The present study aims to evaluate the current cybersecurity attack landscape and the implemented controls for the water infrastructure in Australia. Furthermore, a global assessment of cybersecurity developments is undertaken to compare against Australia's recent cybersecurity water infrastructure developments.

2. Methodology

A systemic review approach was used to assess the research on cybersecurity risks and challenges for cyber–physical systems in the water sector of Australia and to find out areas that need attention. To achieve this objective, several research articles were studied and evaluated using a set of research questions. When conducting the review, the Preferred Reporting Items for Systematic Reviews (PRISMA) guidelines were followed, as shown in Figure 1 [25,26].

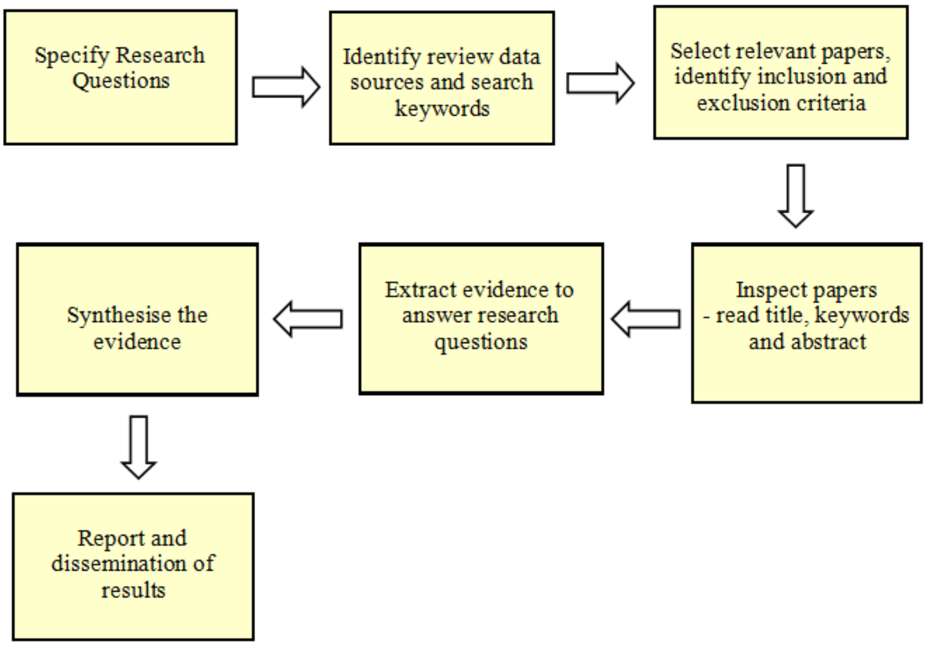
Specify Research Questions
Identify review data sources and search keywords
Select relevant papers, identify inclusion and exclusion criteria
Inspect papers - read title, keywords and abstract
Extract evidence to answer research questions
Synthesise the evidence
Report and dissemination of results

Figure 1. The systematic review process [25].

The following research questions are formed to conduct the SLR:

- RQ1: What are the current cybersecurity threats and control systems in the water sector of Australia?
- RQ2: How do the cybersecurity management systems of the water sector in Australia compare to other countries?
- RQ3: What are the existing research developments around cybersecurity management for water infrastructure?
- RQ3.1: How did the number of publications change over the years?
- RQ3.2: What is the geographic distribution of these studies (across countries)?
- RQ3.3: What is the distribution of the relevant research authority (academic, governmental, and industry) in this study area?
- RQ3.4: What are the most globally cited research studies in this area?
- RQ3.5: What are the target venues for publishing these studies?
- RQ3.6: What are the limitations of the existing studies and the directions for future research?
- RQ3.7: What objective functions and evaluation metrics have the existing studies applied to deal with cybersecurity issues in water infrastructure?

Moreover, a bibliometric analysis was conducted to find out the existing research developments around cybersecurity management for water infrastructure. In the first phase, keywords related to cybersecurity challenges in critical infrastructure systems were selected to search the relevant databases. The keywords that were used to search the articles from the scientific database (Scopus) were as follows: cyber security; cybersecurity; information security; cyber-physical security; cyber-physical attack; security attack; cyber threats; cyber vulnerabilities; cyber challenges; smart water system. Altogether, 481 research articles were found from the search, and 271 were manually sorted out based on their relevance to the research questions. The eligible documents were then analysed to extract the expected observations for this article.

3. Results

This section synthesises the selected literature for this SLR and answers the defined research questions for this study.

3.1. Cybersecurity Challenges for Water Infrastructure in Australia

The cybersecurity of critical infrastructure is one of Australia's top priority sectors. Studies show that Australian organisations spend about AU$1.37–AU$1.74 billion per year on the security of critical infrastructure. In addition, recurring security incidents cause substantial financial losses, estimated at AU$ 595–AU$ 649 million in 2006 [27].

In Australia, network architectural ICS systems have been developed since the 1960s for interconnections of vast distances across the country. Their application has shifted the conventional hardware and software platforms to a new standard level [28].

Due to the vast size of Australia, highly distributed SCADA systems are used to control the geographically scattered water infrastructure systems, which are often dispersed over thousands of square kilometres, where centralised data collection and control (such as flow rates and pressures) are vital to system performance. In addition, field devices perform local operations such as closing and opening breakers and valves, collecting data from sensors, and monitoring alarm systems. Moreover, in water infrastructure, DCSs work as integrated control architecture systems comprising a regulatory level of control, and in turn supervising multiple incorporated sub-systems that control each aspect of a local operation [29]. Other vital elements of ICS systems include:

- Remote terminal unit (RTU): The RTU is a wireless telemetry unit specially constructed to maintain distant SCADA stations. RTUs are field instruments often set with radio interconnections to assist isolated places where wire-based connections are absent.
- Programmable logic controller (PLC): The PLC is a small processor constructed to accomplish logical operations through the use of electric hardware (switches, transmitters, and timers). PLCs are involved in managing complex procedures in DCS and SCADA systems.

Previously, the industrial control systems (SCADA, DCS, PLC) used in many of Australia's critical infrastructure systems were considered reliable, as they protected distant infrastructure systems from being physically harmed. For example, introducing remote control systems into water dams is believed to protect against the illegal release of dam water, since manually operable valves and switches are not accessible. However, linking SCADA systems to commercial computer systems makes them more vulnerable to cyber-attacks that implant faulty data through remote access via dial-up modems [30,31].

The number of emerging terrorist organisations and advanced information communication technologies (ICTs) have intensified the SCADA security threats ever since. The development of Internet-based communication systems such as web-enabled screens and ethernet communications have made SCADA systems more vulnerable and increased the chance of cyber-attacks [32,33].

According to Mays [34], the advancement of transmission systems and the combination of multiple systems and communications protocols designed for SCADA systems makes them easily accessible for attackers, since security issues were not considered during their early development and implementation. Even the electronic chips used in some cybersecurity systems do not have the computing ability to encode the transmission for security purposes [35]. Furthermore, many legacy cybersecurity systems are incompatible with improved security systems such as intrusion detection devices and advanced encryption systems. This is a common reason for frequent cyber-attacks in critical infrastructure systems such as water infrastructure. Another important reason is the availability of security system manuals and documents [33]. According to Pollet, we are living in a time "when the technical knowledge and motivation are beginning to meet". Hacker groups now have the knowledge, instrumental setup, and skills to cause harm via a computer. It is also possible that at some point, hackers could be tempted by terrorists to engage in cybercrime, including cyber terrorism, for money. These vulnerabilities evidently increase the attack possibilities by different hacking groups or terrorist groups, as they are well aware of the weaknesses of these systems.

Many attack detection strategies have been proposed to defend against security challenges in water infrastructure. For example, the ensemble methodology, artificial neural network (ANN) model, long short-term memory recurrent neural network (LSTM-RNN) model, and autoencoder neural networks (AE) are some of the popular methods proposed in the literature, as identified by [3].

3.2. Common Cybersecurity Vulnerabilities and Threats in Water Infrastructure Systems

The US Department of Energy conducted a research program in 2006 known as Test Bed (NSTB) to detect significant vulnerabilities in critical infrastructure systems. The primary purpose of the research was to investigate and assess the security performances of different sizes and types of SCADA systems with complex networks. The study identified ten categories of vulnerabilities, which are discussed in Table 1 below.

Table 1. The vulnerabilities detected from the NSTB assessment [31,35].

Category	Description
Unencrypted (Clear Text) Communications	Unencrypted communications are usually seen in network traffic, which allows a correctly positioned attacker to see a legal user's network traffic, record and observe their communications, and uncover any information the legal user supplies. Additionally, an attacker is able to change the traffic and can use the application as a platform for attacks.
Account Management	Users' accounts that uses easily predicted usernames and passwords; sometimes, attackers can code some tough usernames and passwords that have been defined in records or extracted from binary systems or arrangement files. Additionally, the policies related to password protection are weak.
Weak or No Authentication	Little authentication or the absence of authentication of communication between hosts increases susceptibility to cyber-attacks.
Coding Practices	Dismantling or re-arranging of existing code that causes malicious input of data because of potentially insecure coding styles (specifically due to loop control and buffer management).
Unused Services	Services with ordinary susceptibilities were running in the hosts' system; the need for maintenance was not recommended in the default system.
Network Addressing	Network address protocols (DNS, etc.) were vulnerable to scamming or other circumvention systems.
Scripting and Interface Programming	Archive and other records (Perl, etc.) could be manipulated with malevolent insert or other methods.
Unpatched Components	Old software modules that contained known available vulnerabilities required by the configuration.
Web Servers and Clients	Faulty configured web servers may allow directory traversal or file alteration issues.
Boundary Protection	Misconfigured access control lists may happen from links originating from outside the SCADA boundary; the firewalls contained excess open ports.
Enumeration	Attackers may use the available information revealed from web servers and other networks services.

The threats discovered by Fink et al. [34] revealed the risks that critical infrastructure control systems such as SCADA are presently facing since these systems were incorporated into the cyberspace. Recently, other studies also revealed similar vulnerabilities in security systems for large water utilities, which included the following:

- Always being logged-in to the operator station, even in the absence of an operator at the workstation, limiting the authentication activity;
- It is easy to get access to the security equipment;

- There is insecure access to the security network from distant or isolated locations through dial-up modem lines or digital subscriber lines (DSLs);
- Direct or indirect exposure to the Internet system makes the security networks more vulnerable;
- The absence of a firewall or weak or unverified firewall configurations;
- Unsupervised system event logs;
- The absence of intrusion detection systems;
- The absence of routinely maintained operating and security system software;
- Insecure network and router configurations [31].

3.3. Australian Cybersecurity Management Initiatives and Standards for Water Infrastructure

In Australia, the water infrastructure owners and operators follow a very minimal number of security standards to address cybersecurity vulnerabilities compared to overseas cybersecurity standards. However, the critical infrastructure asset owners and operators in Australia have been assisted by different initiatives developed by the government.

The Australian government has developed the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) to allow critical infrastructure owners and operators to share information on emerging issues relating to system attacks and vulnerabilities, operational continuity, consequence management, the safeguarding of key infrastructural sites from attack or damage, and threats (chemical, biological, and radiological) to water and food supplies [36]. This network has several critical infrastructure advisory councils comprising IT security experts and the SCADA community to emphasise the need for systems security to lessen vulnerabilities and threats. Figure 2 shows that the TISN network's key focus is on the protection of Australia's critical infrastructure systems. Despite some vulnerabilities and weaknesses, TISN has proved its effectiveness in critical infrastructure protection for Australia [37].

The central Commonwealth Government of Australia has also established an umbrella of training, financial aid, support, and data to collaborate among local and state governments and different levels of stakeholders (private sector, voluntary organisations, and individual households). The Victorian Government of Australia led the way by integrating the water sector as an essential service into a parliamentary act known as the Terrorism (Community Protection) Act 2003 in 2006 [38]. According to this act, it is now an obligatory requirement for water organisations to:

- Prepare a risk management plan regarding the terrorist act;
- Conduct an audit on this plan on an annual basis;
- Check the plan annually and prepare a crisis simulation exercise.

All Australian states are now following the Victorian approach with the aim strengthening the protection of water and wastewater CI and services.

As the private sector of Australia is not particularly committed to protecting SCADA systems, in 2005, the Computer Network Vulnerability Assessment Program (CNVA) was developed to reduce the SCADA system's weaknesses. This program was developed to enhance the effectiveness of the Trusted Information Sharing Network (TISN) for Australia's water infrastructure protection by identifying critical threats to the system and checking the performance of the system to control misuse [40]. The program provides dollar-for-dollar grants to assist the owners and operators of water infrastructure systems to:

- Detect key exposures within ICT systems and assess the ability of the systems to withstand exploitation;
- Analyse the safety implications of strategic changes to the infrastructure;
- Evaluate the related physical and personnel safety issues.

In addition, the CNVA program ensures the suitability of the policies, processes, and infrastructure for the organisation's existing environment. It also offers an opportunity to upgrade different approaches to safeguard critical services under various conditions and situations [41].

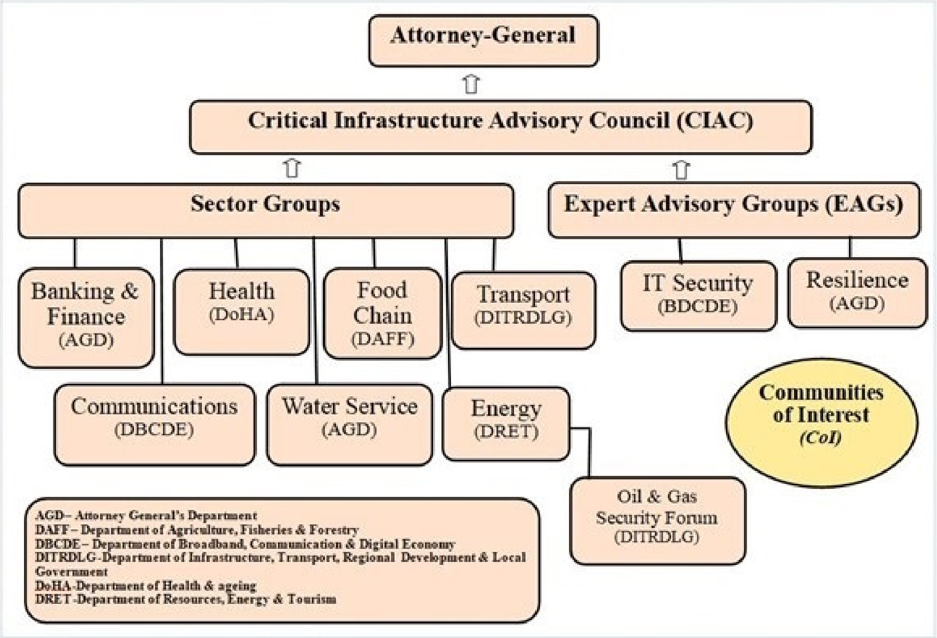
Attorney-General
Critical Infrastructure Advisory Council (CIAC)
Sector Groups
Expert Advisory Groups (EAGs)
Banking & Finance (AGD)
Health (DoHA)
Food Chain (DAFF)
Transport (DITRDLG)
IT Security (BDCDE)
Resilience (AGD)
Communications (DBCDE)
Water Service (AGD)
Energy (DRET)
Communities of Interest (CoI)
Oil & Gas Security Forum (DITRDLG)
AGD– Attorney General's Department
DAFF – Department of Agriculture, Fisheries & Forestry
DBCDE – Department of Broadband, Communication & Digital Economy
DITRDLG-Department of Infrastructure, Transport, Regional Development & Local Government
DoHA-Department of Health & ageing
DRET-Department of Resources, Energy & Tourism

Figure 2. The Australian government's structure for the Trusted Information Sharing Network (TISN) [39].

GovCERT (Government national computer emergency response team) is also another "plans and policy"-based scheme launched by the Australian government to protect Australia from severe data breaches. The main aim of this scheme is to incorporate plans and policies together to prepare and safeguard the national database infrastructure from a cyber-attack or potential cyber terrorism. GovCERT is responsible for:

- Coordinating GovCERT with foreign governments regarding cybersecurity issues in Australia's critical infrastructure systems, such as its water infrastructure;
- Incorporating the Australian government's policies with the private sector's policies for securing and overcoming cyber-based attacks;
- Providing cash grants to private sector organisations to carry out safety assessments of their systems and networks.

Furthermore, another online portal has been set up by the Australian government to enable collaboration between government organisations, academic institutions, and water infrastructure owners and operators to prevent cyber terrorism [31]. Lastly, the cross-sector-based SCADA Risk Management Framework (RMF) was introduced to assist water infrastructure system owners in managing risks.

3.4. *Overseas Cybersecurity Management Standards for Water Infrastructure*

Recently, several security standards have been developed and implemented worldwide to cope with cybersecurity challenges. The use of digital encryption standards is a popular approach to safeguarding water infrastructure systems against cyber terrorism. However, many old water infrastructure system owners are facing difficulties in adopting new technologies to secure their water infrastructure systems.

Likewise, the National Institute of Standards and Technology (NIST) has developed standards and process control safety requirement forums to protect water infrastructure, as well as the Industrial Control Systems Security (SP 800-82) framework [41]. This framework provides a set of core activities that can be used to reach specific cybersecurity goals. These activities include identifying, protecting, detecting, responding, and recovering.

Another standard ISA-SP99 was developed by the Instrumentation Systems and Automation Society (ISA) for systems security control in critical infrastructure. ISA-SP99 forms principles to build an automatically secure control system, as well as to assess the security performance of a system. In addition, in 2005, the National Infrastructure Security Coordination Centre (NISCC) of the UK established a security guide for risk management and firewall deployment for critical infrastructure systems [42].

Although several security standards have been developed and implemented worldwide to protect critical water infrastructure systems, the number of cyber threats to these platforms continues to rise. The annual Cyber Threat Report from the Australian Cyber Security Centre (ACSC) revealed that cyber-attacks continue to alarmingly increase throughout the world, which affects the economic status and reputation of critical infrastructure service organisations [43,44].

Sun et al. [44] noted that it is impossible to evaluate every security standard due to the different complex challenges and circumstances of a nation and its organisations. It is well known that cyber threats and cyber terrorism are advancing concurrently with the advancement of cybersecurity. This indicates that the system security of critical infrastructure, such as water infrastructure, needs to be upgraded with contemporary security standards.

3.5. Existing Research Developments around Cybersecurity Management for Water Infrastructure

A systematic review has been carried out for the current study. The critical information regarding the review analysis is presented in Table 2. A total of 271 studies were sorted manually from 210 sources over the timespan of 2003–2023, clearly demonstrating that the cybersecurity challenges for critical infrastructure issues emerged at the beginning of the 21st century. Among the 271 studies, 128 were found to be conference papers, which was more than the number of journal articles.

Table 2. The main information and statistics used in this study (2003–2023).

Description	Results	Description	Results
Main Information		Document Contents	
Timespan	2003–2023	Keywords Plus (ID)	2001
Sources (Journals, Books, etc.)	210	Author's Keywords (DE)	886
Documents	271	Authors	
Average years from publication	3.91	Authors	916
Average citations per documents	16.3	Author Appearances	1037
Average citations per year per doc	3.077	Authors of single-authored documents	29
References	10,126	Authors of multi-authored documents	887
Document Types		Author Collaborations	
article	99	Single-authored documents	31
book	2	Documents per Author	0.296
book chapter	29	Authors per Document	3.38
conference paper	128	Co-Authors per Documents	3.83
review	13	Collaboration Index	3.7

Figure 3 shows the number of publications over time. The earliest study on cybersecurity challenges in critical infrastructure systems was in the year 2003. The figure shows that from 2003 to 2009, a limited amount of research was published, which then began to increase from the year 2010 and reached its highest peak (44) in the year 2022. Answering RQ3.1, there has been growing attention given to the cybersecurity issues of water infrastructure systems over time, likely because of the advent of new technologies for water resource systems and subsequent efforts to make use of them.

Table 3 presents the numbers of studies per country across the world. From the table, it can be seen that the USA has published the highest number of studies (178), followed by China (136), India (111), South Korea (53), and the UK (51). Australia attained 6th position in terms of the number of publications (46).

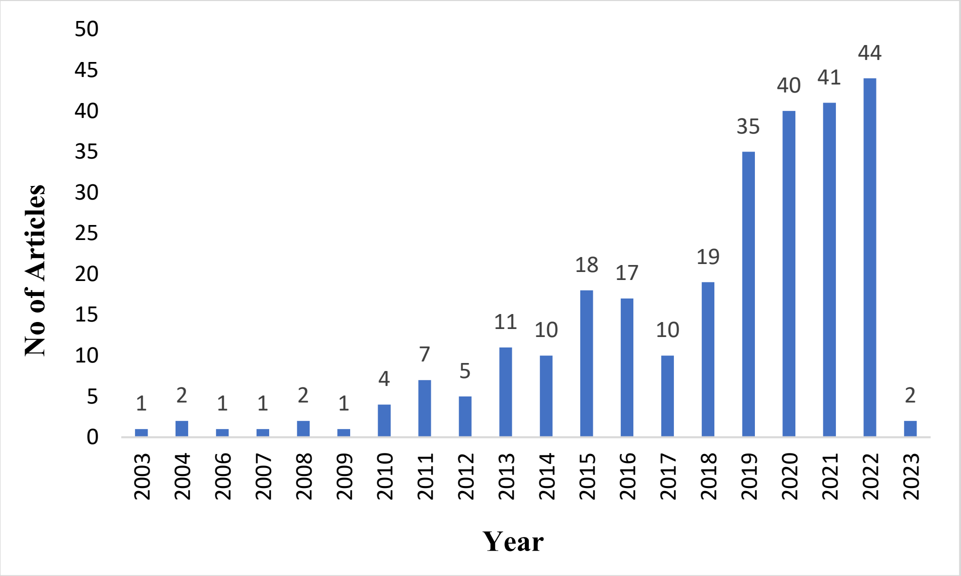

Figure 3. The numbers of publications change over the years.

Table 3. The research country's production rates over time.

SL.	Region	Freq	SL.	Region	Freq
1	USA	178	11	FRANCE	25
2	CHINA	136	12	SAUDI ARABIA	23
3	INDIA	111	13	ROMANIA	17
4	SOUTH KOREA	53	14	MALAYSIA	16
5	UK	51	15	ISRAEL	14
6	AUSTRALIA	46	16	MEXICO	14
7	ITALY	36	17	KENYA	13
8	SPAIN	35	18	PAKISTAN	13
9	GERMANY	30	19	SOUTH AFRICA	11
10	SINGAPORE	30	20	AUSTRIA	9

Figure 4 represents the research distribution based on the corresponding authors' country of origin. The figure also shows whether the authors are from single or multiple countries. From the figure, it can be observed that the USA has the highest number of studies (29), of which 22 are SCPs (intra-country collaborations) and seven are MCPs (inter-country collaborations). China has the 2nd highest number of studies (26), of which 20 are SCPs and 6 are MCPs. Australia is the 6th highest country in terms of the corresponding authors, which has 7 SCPs and 1 MCP study.

Figure 5 represents research on the cybersecurity issues for critical water infrastructure in recent years (2017–2020). The figure illustrates that between 2017 and 2018, Australia, Italy, and Pakistan performed some collaborative work with other countries. From mid-2018 to mid-2020, the USA, China, South Korea, Malaysia, and Russia contributed significant research in this area by collaborating with several countries worldwide. However, in 2020, India, Taiwan, and Denmark emerged as new countries focusing on cybersecurity issues for critical water infrastructure.

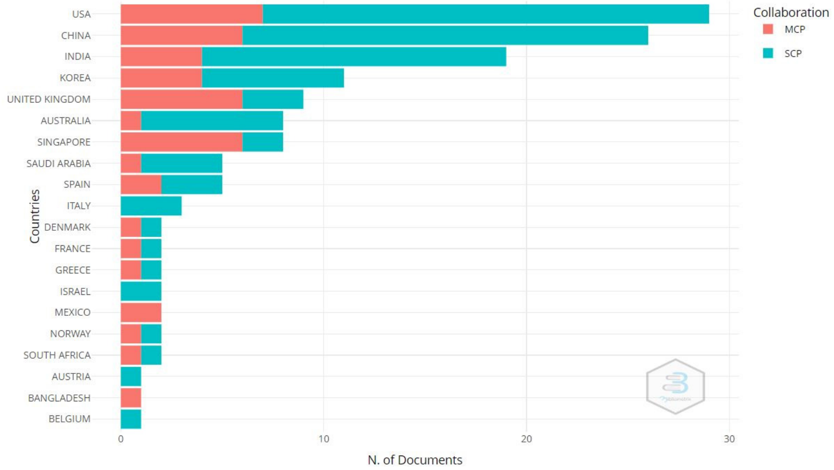

Figure 4. The most relevant countries based on the corresponding authors (SCPs (single country publications) and MCPs (multiple-country publications)).

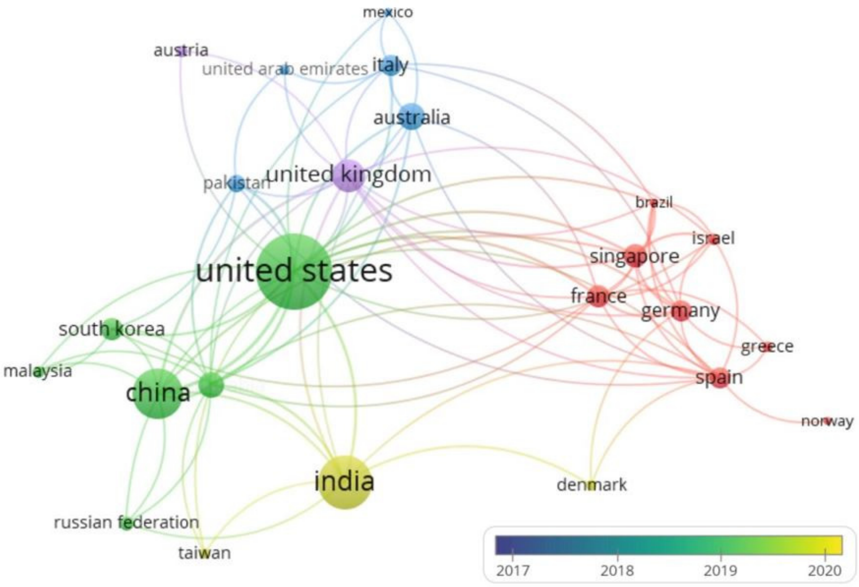

Figure 5. The geographic distribution of the articles over time.

Table 3 and Figures 4 and 5 answer RQ3.2 based on the geographical distribution of the research. Some additional information regarding RQ3.2 is provided in the Supplementary Materials (Table S1).

Figure 6 illustrates the answer to RQ3.3. From the figure, it is clear that approximately 94% of the research has been conducted by academics. Government agencies and private organisations have carried out only 3% of the research each. Interestingly, no research studies or documents that were collaboratively written by authors from water institutions or water organisations could be found.

The topmost globally mentioned and leading articles on cybersecurity issues for critical water infrastructure in Australia are shown in Table 4 below. RQ3.4 is answered in this table. The table clearly shows that urban water management, smart metering, and cybersecurity in Australia's water sectors have gained the utmost attention (14 out of the top 15 articles are related to water sector management and cybersecurity issues). Fielding et al. [45] published the most cited article on strategies to promote urban water demand management in the *Journal of Environmental Management*. The article not only discussed the security issues in water systems but also covered the smart metering technologies in urban water demand management. The article by Stewart et al. [46] is the 2nd most cited article published in the *Australian Planner*, which discussed web-based smart metering technologies in water planning.

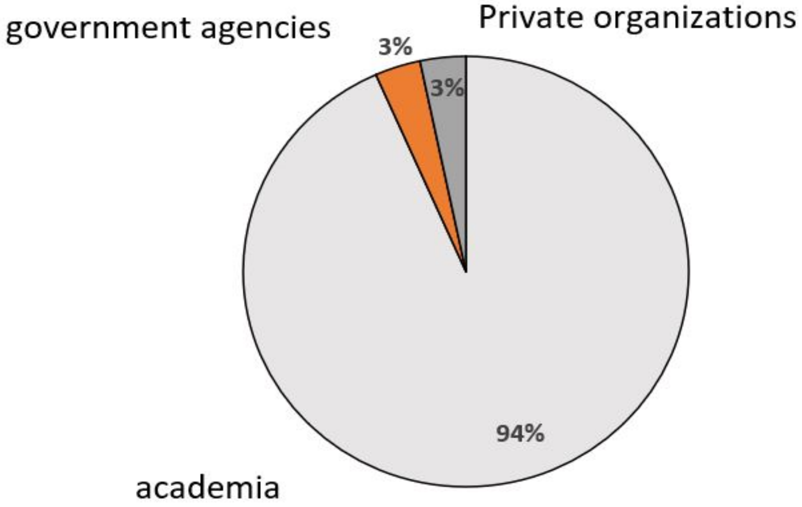

Figure 6. The distribution of the relevant research authorities.

Table 4. Top 15 most global cited documents in Australia (R = rank; TC = total citations; NTC = normalized total citations).

R	Author	Articles	Journals	TC	TC/Year	NTC
1	Fielding KS, 2013	An experimental test of voluntary strategies to promote urban water demand management	*J. Environ. Manage.*	265	26.5	4.34
2	Stewart RA, 2010	Web-based knowledge management system: Linking smart metering to the future of urban water planning	*Aust Planner*	111	8.54	1.00
3	Cole G, 2013	Smart meter enabled disaggregation of urban peak water demand: Precursor to effective urban water planning	*Urban Water J.*	69	6.90	1.88
4	Gurung TR, 2015	Smart meter enabled water end-use demand data: Platform for the enhanced infrastructure planning of contemporary urban water supply networks	*J. Cleaner Production*	59	7.38	2.42
5	Gurung TR, 2014	Smart meters for enhanced water supply network modelling and infrastructure planning	*Resources, Conservation and Recycling*	59	6.56	2.46
6	Luiijf E, 2013	Nineteen national cybersecurity strategies	*Int. J. of Critical Infrastructure systems*	59	5.90	1.61

Table 4. *Cont.*

R	Author	Articles	Journals	TC	TC/Year	NTC
7	Liang G, 2019	A framework for cyber topology attacks: Line-switching and new attack scenarios	*IEEE Transactions on Smart Grid*	57	14.25	3.86
8	Nguyen KA, 2015	Intelligent autonomous system for residential water end use classification: Autoflow	*Applied Soft Computing Journal*	50	6.25	2.05
9	Nguyen KA, 2014	An autonomous and intelligent expert system for residential water end-use classification	*Expert Systems with Applications*	43	4.78	1.79
10	Moglia M, 2018	Promoting water conservation: Where to from here?	*Water (Switzerland)*	33	6.60	3.79
11	Andreasson K, 2015	Digital divides: The new challenges and opportunities of e-inclusion	*Digital Divides: The New Challenges and Opportunities of e-Inclusion*	29	3.63	1.19
12	Thiyagarajan K, 2020	Robust Sensor Suite Combined with Predictive Analytics Enabled Anomaly Detection Model for Smart Monitoring of Concrete Sewer Pipe Surface Moisture Conditions	*IEEE Sensors*	27	9.00	5.10
13	Vakilifard N, 2019	An interactive planning model for sustainable urban water and energy supply	*Applied Energy*	26	6.50	1.76
14	Talebpour MR, 2014	Water and energy nexus of residential rainwater tanks at an end-use level: Case of Australia	*Energy and Buildings*	25	2.78	1.04
15	Parvin S, 2013	Multi-cyber framework for availability enhancement of cyber–physical systems	*Computing*	24	2.40	0.65

Table 5 answers RQ3.5 regarding identifying the target venues for publishing cybersecurity management for water infrastructure studies. The ACM International Conference Proceeding Series is the leading and most popular journal for publishing studies on the cybersecurity challenges related to critical water infrastructure. Among the journals, *IEEE Access*, *Water (Switzerland)*, *Electronics*, *Advances in Intelligent Systems and Computing*, *IEEE Internet of Things*, and *Journal of Water Resources Planning and Management* are the most common publications for publishing cybersecurity challenges in the critical water infrastructure area.

Table 5. The most relevant sources of research.

SL.	Sources	Articles
1	*ACM International Conference Proceeding Series*	6
2	*IEEE Access*	6
3	*Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*	6
4	*Water (Switzerland)*	6
5	*Electronics (Switzerland)*	5
6	*Advances in Intelligent Systems and Computing*	4
7	*IEEE Internet of Things*	4
8	*Journal of Water Resources Planning and Management*	4
9	*Communications in Computer and Information Science*	3
10	*IET Conference Publications*	3
11	*International Journal of Critical Infrastructure Protection*	3
12	*Procedia Engineering*	3
13	*Sensors*	3
14	*Sustainable Cities and Society*	3
15	*Wireless Personal Communications*	3
16	*Advanced Sciences and Technologies for Security Applications*	2
17	*Applied Sciences (Switzerland)*	2
18	*Computers And Security*	2
19	*IEEE International Conference on Communications*	2
20	*IEEE Sensors*	2

A thematic map (Figure 6) was prepared using author-nominated keywords and ten clusters of research themes to answer RQ3.6. We set the following criteria for creating the thematic map: the top 250 author-nominated keywords and a minimum cluster frequency rate of 5 with three labels for each cluster. The degree of development (x-axis) and the relevance degree (y-axis) measure the development of the selected theme and the importance of the chosen theme, respectively [47,48]. Figure 7 shows that 'artificial intelligence', 'machine learning', 'rainwater', and 'ground water' are motor themes, which implies that they are well-developed research fields. The figure also shows that the cluster that includes 'cyber security', 'deep learning', 'Australia', and 'cyber warfare water balance' contains important research fields that have not been fully developed until now. Likewise, the clusters that include 'cyber security', 'policy', 'cyber security industry', 'water end use', and 'critical infrastructure' are critically important and demand more attention for research in these areas. 'Smart water network' is the only cluster in the niche theme, which is well-developed but isolated from the other areas. There are two clusters that are emerging themes, which include the 'decision support system' and 'urban water supply' clusters and have low density and centrality.

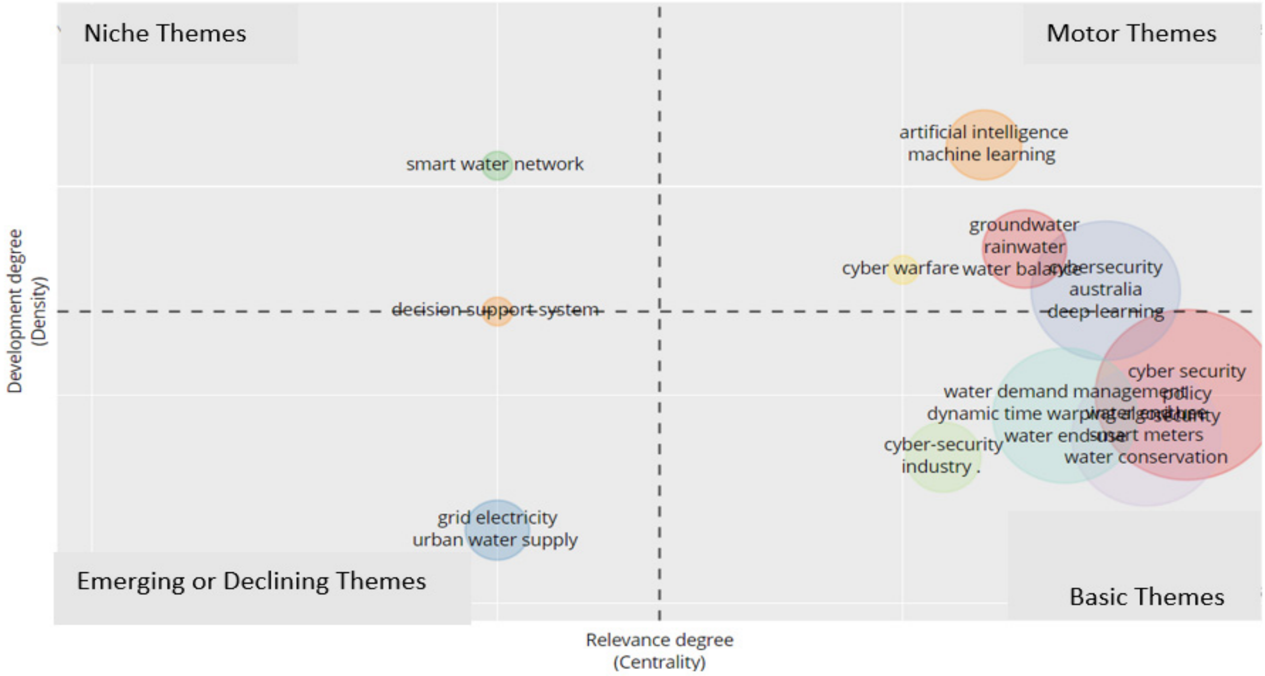

Figure 7. A thematic map of Australia's cybersecurity challenges relating to critical water infrastructure.

3.6. Objective Functions and Evaluation Metrics for Measuring Cybersecurity in Water Infrastructure

This section answers RQ3.7, which discusses the evaluation metrics and objective functions applied in the studied literature. NIST has developed security standards to protect critical infrastructure along with water infrastructure. The analysed studies in this SLR mostly adopted objective functions centred around NIST standards, where the objective functions achieve three goals: confidentiality, integrity, and availability. Confidentiality ensures that no unauthorised party can access sensitive data, while integrity covers the improper modification and alteration of data. Availability ensures that authorised users can access the system and information in a timely and reliable manner [41]. The objective functions assure that the control properties such as the accuracy, responsiveness, rapid disturbance rejection, stability, observability, controllability, safety, and efficiency are met [26].

Most of the existing studies have shown a lack of standard evaluation metrics [26]. Many studies have used traditional machine learning metrics as the performance evaluation metrics for attack detection models of water infrastructure [3]. These metrics are normally the accuracy, precision, recall, F-score, false positive, and false negative values, which fail to report the detection latency [26].

4. Discussion

Germano (2018) [49] illustrated that a cyber-attack on critical water infrastructure operations could cause "outrageous harm to public health and safety and national security risks, consequently resulting in a huge cost for recovery and remediation, as well as big data loss" [49]. The audit reports for water and energy systems in Queensland, Australia, outline that critical water infrastructure systems are increasingly becoming among the most targeted for cyber-attacks worldwide [49]. Likewise, an annual assessment by the Department of Homeland Security, USA, reached the same conclusion. The audit reports from Victoria, Australia, concluded that the critical water providers in Australia lacked "a strategic approach to manage cybersecurity risks that incorporates their commercial and control system environments and associated guiding industry security standards for control systems" [50]. Moreover, they further stated that although the water suppliers are ramping up their efforts to incorporate some security controls into their systems against cyber threats, the constant advancement of the cyber threat landscape places the utmost emphasis on evaluating and strengthening the water system's security [10].

Usually, critical water infrastructure systems use a number of incorporated technological control systems, including hardware and software, in their operation. In Australia, the system is more complex due to the vastness and remoteness of the infrastructure, which makes the system more prone to cyber threats and attacks. According to the American Water Works Association, a number of basic issues enhance the vulnerability of critical water infrastructure to cyber-attacks, such as inadequate and low-grade network protection instruments and a lack of firewall and antivirus protection [50].

The critical water infrastructure faces other threats associated with the control system and equipment companies' services, including the vendor or manufacturer's access to the water system for the purposes of updating the system, searching for faults, and performing remote maintenance. Failure to change the retailer's default settings, upgrade the security measures, and consistently patch up the systems and software can introduce more vulnerabilities or lead to any existing vulnerabilities being exploited. The negligence of water system owners and operators in assessing cybersecurity risks can also cause the system to be more vulnerable. According to the American Water Works Association, "The reality and prevalence of cyber risk mandates that organisations and their leaders not only take meaningful action to prevent and detect harms, but also have a tested plan for responding swiftly and effectively when cyber incidents do occur. Failing to address cybersecurity risk in a proactive way can have devastating results".

An array of technological and procedural standard security measures can assist in securing water systems against many cyber-attacks [3]. A significant cause of cybersecurity issues in critical water infrastructure is the lack of well-defined and documented tasks and responsibilities for employees to manage the security of the water systems, as stated by the Victorian Auditor-General's Office [51].

A recent survey by Hassanzadeh et al. [16] revealed a range of threats and circumstances from a review of fifteen cybersecurity incidents in Australia's critical water infrastructure sector, ranging from the Maroochy Shire Sewage Treatment Plant attack in 2001 to the ransomware attack on the Riviera Beach Water Utility in 2019. The study revealed that the sheer variety of the systems, the sophisticated and diverse attacking techniques, and the array of consequences related to these incidents create an urgent need for comprehensive and strategic approaches for risk assessment and mitigation, alertness, immediate response, and data recovery processes to deal with these emerging challenges. The study also emphasised the need for expert training and human resource development for individuals who are capable of constantly assessing the system's security and identifying threats in the commercial network infrastructure and SCADA systems used in water infrastructure [16].

5. Conclusions

Smart water systems have become an integral part of modern infrastructure. These systems will enable the use of recycled water resources to overcome the scarcity of clean water at the global level. However, these systems are prone to growing cyber-attacks, like any other critical infrastructure system. As IoT technology is advancing, water infrastructure systems in Australia are gradually using smart systems technology, making them more susceptible to cyber-attacks. A systematic review was conducted to assess the current cybersecurity challenges related to the critical water infrastructure in Australia. The key the findings of the SLR are as follows:

- Water infrastructure systems in Australia are frequently facing cyber-attacks due to their complex nature;
- Many attacks remain undetected or unreported, or else undisclosed to safeguard consumers' trust and the service providers' reputations;

- Although the Australian government is taking different initiatives (policies or strategies and financial aid) at the federal, state, and local levels to collaborate with the public and private sectors to protect Australia's critical water infrastructure, there are still some significant gaps in addressing cyber risks and implementing adequate security controls;
- There is an urgent need for expert training and human resource development for individuals who are capable of constantly assessing the system's security and identifying threats in the commercial network infrastructure, as well as in the SCADA systems used in the water infrastructure.

Overall, this SLR has identified that the water infrastructure plays a crucial role in attaining the sustainable development of a nation through safeguarding and ensuring a safe water supply. Therefore, to ensure that secured and uninterrupted water distribution is possible, it is an important obligation to protect the database and sub-systems that form the backbone of the water control system.

Supplementary Materials: The following are available online at https://www.mdpi.com/article/10.3390/w15010168/s1, Table S1: Corresponding authors country.

Author Contributions: Conceptualization, S.J., A.B. and F.F.; methodology, S.J.; software, S.J.; validation, S.J., A.B. and F.F.; formal analysis, S.J.; investigation, S.J.; resources, S.J., A.B. and F.F.; writing—original draft preparation, S.J.; writing—review and editing, S.J., A.B., F.F. and F.A.; visualization, S.J.; supervision, A.B. and F.F.; project administration, A.B. and F.F.; funding acquisition, A.B. All authors have read and agreed to the published version of the manuscript.

Funding: No other funding excerpt publication funding from Western Sydney University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Williams, A. Beyond 2000: The Rise of Australian Cyber Warfare Capability. In Proceedings of the International Conference on Cyber Warfare and Security, Towson, MD, USA, 9–10 March 2020; Academic Conferences International Limited: Manchester, UK, 2020; p. 549-XVIII. Available online: https://www.proquest.com/docview/2455894288?pq-origsite=gscholar&fromopenview=true (accessed on 23 October 2022).
2. Shamir, U.; Salomons, E. Optimal Real-Time Operation of Urban Water Distribution Systems Using Reduced Models. *J. Water Resour. Plan. Manag.* **2008**, *134*, 181–185. [CrossRef]
3. Addeen, H.H.; Xiao, Y.; Li, J.; Guizani, M. A survey of cyber-physical attacks and detection methods in smart water distribution systems. *IEEE Access* **2021**, *9*, 99905–99921. [CrossRef]
4. Gleick, P.H. Water and terrorism. *Water Policy* **2006**, *8*, 481–503. [CrossRef]
5. Mutchek, M.; Williams, E. Moving towards sustainable and resilient smart water grids. *Challenges* **2014**, *5*, 123–137. [CrossRef]
6. Gonzalez-Vidal, A.; Cuenca-Jara, J.; Skarmeta, A.F. IoT for water management: Towards intelligent anomaly detection. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 858–863.
7. Hopman, V.; Kruiver, P.; Koelewijn, A.; Peters, T. How to create a smart levee. In Proceedings of the 8th International Symposium on Field Measurements in GeoMechanics 2010, Berlin, Germany, 12–16 September 2011.
8. Li, J.; Yang, X.; Sitzenfrei, R. Rethinking the framework of smart water system: A review. *Water* **2020**, *12*, 412. [CrossRef]
9. Priya, S.K.S.G.; Revathi, T. Design of smart sensors for real time drinking water quality monitoring and contamination detection in water distributed mains. *Int. J. Eng. Technol.* **2018**, *7*, 47–51. [CrossRef]
10. Skiba, R. Water Industry Cyber Security Human Resources and Training Needs. *Int. J. Eng. Manag.* **2020**, *4*, 11–16. [CrossRef]
11. Sun, B.; Ahmed, F.; Sun, F.; Qian, Q.; Xiao, Y. Water quality monitoring using STORM 3 data loggers and a wireless sensor network. *Int. J. Sens. Netw.* **2016**, *20*, 26–36. [CrossRef]
12. Gleick, P.H. The water conflict chronology. In *The World's Water 2004–2005: The Biennial Report on Freshwater Resources*; Gleick, P.H., Ed.; Island Press: Covelo, CA, USA, 2004; pp. 234–255.

13. *Presidential Decision Directive: Critical Infrastructure Security and Resilience*; Technical Report PPD-21; The White House: Washington, DC, USA, 2013.
14. White House. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*; Technical Report; 2017. Available online: https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (accessed on 23 October 2022).
15. ICS-CERT. *NCCIC/ICS-CERT Year in Review: FY 2015*; U.S. Department of Homeland Security Industrial Control Systems-Cyber Emergency Response Team: Washington, DC, USA, 2016.
16. Hassanzadeh, A.; Rasekh, A.; Galelli, S.; Aghashahi, M.; Taormina, R.; Ostfeld, A.; Banks, K. A review of cybersecurity incidents in the water sector. *arXiv* **2020**, arXiv:2001.11144v2. [CrossRef]
17. Cava, M.D. Uber to Pay $148 Million over Undisclosed Data Breach that Ex-CEO Paid Hackers to Keep Quiet. USA Today. 2018. Available online: https://www.usatoday.com/story/tech/news/2018/09/26/uber-pay148-million-over-undisclosed-data-breach-ex-ceo-paid-hackers-keepquiet/1432335002. (accessed on 15 August 2019).
18. Rubin, G.T. Many Company Hacks Go Undisclosed to SEC Despite Regulator Efforts. The Wall Street Journal. 2019. Available online: https://www.wsj.com/articles/many-company-hacks-go-undisclosedto-sec-despite-regulator-efforts-11551218919 (accessed on 15 October 2022).
19. Walton, B. Water Sector Prepares for Cyberattacks. Circle of Blue. 2016. Available online: https://www.circleofblue.org/2016/world/water-sector-preparescyberattacks (accessed on 11 October 2022).
20. Australian Government. *Strong and Secure: A strategy for Australia's National Security*; Department of Prime Minster and Cabinet: Barton, Australia, 2013.
21. Slay, J.; Miller, M. Lessons learned from the Marchoory Water Breach. In *Critical Infrastructure Protection*; Springer: Boston, MA, USA, 2008; pp. 73–82.
22. Lehto, M.; Neittaanmäki, P. (Eds.) *Cyber Security: Analytics, Technology and Automation*; Springer: London, UK, 2015; Volume 78, p. 258.
23. Saha, H.N.; Auddy, S.; Chatterjee, A.; Pal, S.; Sarkar, S.; Singh, R.; Singh, A.K.; Sharan, P.; Banerjee, S.; Sarkar, R.; et al. IoT solutions for smart cities. In Proceedings of the 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), Institute of Electrical and Electronics Engineers (IEEE), Bangkok, Thailand, 16–18 August 2017; pp. 74–80.
24. Taormina, R.; Galelli, S.; Tippenhauer, N.O.; Salomons, E.; Ostfeld, A. Characterizing cyber-physical attacks on water distribution systems. *J. Water Resour. Plan. Manag.* **2017**, *143*, 04017009. [CrossRef]
25. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.; The PRISMA Group. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *BMJ* **2009**, *339*, b2535. [CrossRef] [PubMed]
26. Tuptuk, N.; Hazell, P.; Watson, J.; Hailes, S. A systematic review of the state of cyber-security in water systems. *Water* **2021**, *13*, 81. [CrossRef]
27. Richards, K. *Australian Business Assessment of Computer User Security*; Australian Institute of Criminology: Canberra City, Australia, 2009; ISBN 9781921532351.
28. Krutz, R. *Securing SCADA Systems*; Wiley: Indianapolis, IN, USA, 2006.
29. Stouffer, K.; Falco, J.; Scarfone, K. *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*; NIST Special Publication; National Institute of Standards and Technology (NIST), U.S. Department of Commerce: Washington, DC, USA, 2015.
30. Shea, D. Critical Infrastructure: Control Systems and the Terrorist Threat. Congressional Research Services. 2003. Available online: http://www.fas.org/irp/crs/RL31534.pdf (accessed on 1 June 2008).
31. Beggs, C. A holistic SCADA security standard for the Australian context. In Proceedings of the 9th Australian Information Warfare and Security Conference, Perth, Australia, 5–7 December 2008.
32. Khadidos, A.O.; Khadidos, A.O.; Manoharan, H.; Alyoubi, K.H.; Alshareef, A.M.; Selvarajan, S. Integrating Industrial Appliances for Security Enhancement in Data Point Using SCADA Networks with Learning Algorithm. *Int. Trans. Electr. Energy Syst.* **2022**, *2022*, 8685235. [CrossRef]
33. Pollet, J. Developing a Solid SCADA Security Strategy. In Proceedings of the 2nd ISA/IEEE Sensors for Industry Conference, Houston, TX, USA, 19–21 November 2002; pp. 148–156.
34. Mays, L. *Water Supply System Security*; McGraw-Hill: New York, NY, USA, 2004.
35. Fink, R.; Spencer, D.; Wells, R. *Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems Control*; Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy: Washington, DC, USA, 2006.
36. Schneider, A. Parliamentary Joint Committee on the Australian Crime Commission-Inquiry into Cybercrime. Attorneys General Department; 2003. Available online: URL http://www.aph.gov.au/Senate/committee/acc_ctte/cybercrime/submissions/sub21.doc (accessed on 24 August 2008).
37. TISN. Australia's Critical Infrastructure Protection Arrangements. Australian Govt; 2007. Available online: http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~{}TISN+diagram+v.2+Dec+07.pdf/$file/TISN+diagram+v.2+Dec+07.pdf (accessed on 24 August 2008).
38. Victorian Government. *Terrorism (Community Protection) Act 2003*; Parliament of Victoria: Melbourne, Australia, 2003.

39. TISN. Diagram of the TISN. Trusted Information Sharing Network (TISN); 2012. Available online: http://www.tisn.gov.au/Pages/the_tisn.aspx. (accessed on 16 June 2012).
40. TISN. CIP Newsletter. Volume 3, March 2006. Available online: http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~{}Newsletter+March+06.pdf/$file/Newsletter+March+06.pdf (accessed on 10 September 2008).
41. NIST. *Framework for Improving Critical Infrastructure Cybersecurity*; Technical Report; NIST: Gaithersburg, MD, USA, 2017.
42. NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks. Available online: http://www.niscc.gov.uk/niscc/scada-en.html (accessed on 15 October 2022).
43. Australian Cyber Security Centre. ACSC Annual Cyber Threat Report. September 2020. Available online: https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-CyberThreat-Report2019-20.pdf (accessed on 10 October 2022).
44. Sun, N.; Zhang, J.; Rimba, P.; Gao, S.; Xiang, Y.; Zhang, L.Y. Data-driven cybersecurity incident prediction: A survey. *IEEE Commun. Surv. Tuts.* **2018**, *21*, 1744–1772. [CrossRef]
45. Fielding, K.S.; Spinks, A.; Russell, S.; McCrea, R.; Stewart, R.; Gardner, J. An experimental test of voluntary strategies to promote urban water demand management. *J. Environ. Manag.* **2013**, *114*, 343–351. [CrossRef]
46. Stewart, R.A.; Willis, R.; Giurco, D.; Panuwatwanich, K.; Capati, G. Web-based knowledge management system: Linking smart metering to the future of urban water planning. *Aust. Plan.* **2010**, *47*, 66–74. [CrossRef]
47. Cobo, M.J.; López-Herrera, A.G.; Herrera-Viedma, E.; Herrera, F. An approach for detecting, quantifying, and svisualising the evolution of a research field: A practical application to the Fuzzy Sets Theory field. *J. Informetr.* **2011**, *5*, 146–166. [CrossRef]
48. Cobo, M.J.; López-Herrera, A.G.; Herrera-Viedma, E.; Herrera, F. Science mapping software tools: Review, analysis, and cooperative study among tools. *J. Am. Soc. Inf. Sci. Technol.* **2011**, *62*, 1382–1402. [CrossRef]
49. Germano, J.H. *Cybersecurity Risk & Responsibility in the Water Sector*; AWWA: Denver, CO, USA, 2018.
50. American Water Works Association. 2019 AWWA State of the Water Industry Report. 2019. Available online: https://www.awwa.org/Portals/0/AWWA/ETS/Resources/2019_STATE%20OF%20THE%20WATER%20INDUSTRY_post.pdf (accessed on 15 October 2022).
51. Victorian Auditor-General's Office. *Security of Water Infrastructure Control Systems*; Victorian Government Printer: Melbourne, Australia, 2019.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.