Defending the Water and Wastewater Sector: Unveiling Advanced Persistent Threats and Tactics, Techniques, and Procedures for Enhanced Defense

by

Jonathan Brendese

A Capstone Project Submitted to the Faculty of

Utica University

May 2024

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in

Cybersecurity

Abstract

Advanced Persistent Threats (APTs) pose an increasingly severe threat to U.S. critical infrastructures (CIs), including the Water and Wastewater Systems (WWS), which are critical to ensuring national security, public health, and economic prosperity. APTs employ tactics, techniques, and procedures (TTPs) to invade U.S. critical infrastructures, obtain information, and exploit vulnerabilities. The increasing reliance on digital infrastructure and interconnected systems exacerbates vulnerabilities to cyberattacks. Nation-state-sponsored APTs utilize various cyberattack methodologies to disrupt operations, compromise data, and disrupt economic and social activities. According to findings, this research demonstrated that ransomware, spear-phishing, denial-of-service attacks, and exploiting outdated systems and software are among the escalating cyberattacks targeting CIs. Also, the research demonstrates the importance of securing U.S. CIs like the WWS against sophisticated APTs to maintain operational continuity and mitigate the expansive range of cyber-related risks.

Keywords: Dr. Cynthia Gonnella, Cybersecurity, Cyberterrorism, Public Health, Economic Stability, Threat Actors, Cyber Threats

Acknowledgments

I want to express my boundless gratitude to my wife, Gianna, who has been my most significant support source throughout the Utica University Cybersecurity Program. Her unwavering support, encouragement, and patience have been invaluable to me, and I am genuinely grateful for her persistent belief in my abilities throughout the program. I would also like to extend my sincere appreciation to Professor Michael Zambotti for his exceptional support and guidance throughout the course of the program. His expertise, dedication, and willingness to assist me have been instrumental in my academic success. Special thanks to Professors Patrick McHarris and David Plude for acknowledging my continued interest in the program and spending additional time with me in order to expand my understanding of various topics and continued growth within the field. To Dr. Cynthia Gonnella, thank you so much for broadening my understanding within the field of research. Your patience and ability to break down material into segments allowed me to become a better researcher and writer. Lastly, I would like to extend my deepest gratitude to Mark Low for his exceptional skills and dedication in editing. Mark's keen eye for detail, commitment to quality, and remarkable ability to improve clarity have truly improved the outcome of this project. As a result of his invaluable contributions, the overall presentation has been greatly improved, and a sense of professionalism and excellence was engendered throughout the process. The success of this project is undeniably due to Mark's expertise and consistent support.

Table of Contents

Statement of the Problem

The purpose of this research was to analyze tactics, techniques, and procedures (TTPs) utilized by Advanced Persistent Threat (APT) groups to target United States (U.S.) critical infrastructures (CIs) and provide insights into mitigations and defense strategies. Why is it essential to analyze current TTPs employed by APT groups for targeting critical infrastructures? Why is protecting U.S. critical infrastructures like Water and Wastewater necessary for our nation's safety, public health, and economic vitality? How do APT groups target the United States' critical infrastructures, and why is understanding and implementing effective defense strategies essential for deflecting these threats?

Cyberattacks have increasingly threatened CIs in the U.S. Robb Shawe, Ph.D., and director of New York Security Consulting Professionals, and Ian McAndrew, who has a Ph.D. in mechanical engineering (2023), authored the article "Increasing Threats to United States of America Infrastructure Based on Cyber-Attacks" and reported an increase in vulnerability as technology advances. A cyberattack on CI, such as the water and wastewater sector (WWS), can pose a significant risk to national security and public safety. Cyberattacks have significantly increased due to the interconnectedness of various systems and the constant advancement of technology (2023).

The Cybersecurity and Infrastructure Security Agency (CISA) described the WWS as one of the 16 CIs of the U.S. and reported that it is vulnerable to cyberattacks (n.d.). CISA stated that approximately 153,000 public drinking water and 16,000 public wastewater treatment systems exist in the U.S. Drinking water and wastewater treatment and service are essential to modern life and the economy. Various attacks can affect the WWS, including but not limited to contamination, physical attacks such as releasing toxic gaseous chemicals, and cyberattacks.

Such attacks could result in severe illnesses, casualties, or denial of service, negatively affecting public health and economic vitality (n.d.).

In his article "Water Industry Cyber Security Human Resources and Training Needs," Richard Skiba (2020), an electrical engineer for Caterpillar, reported the growing number of cyberattacks on the WWS. Skiba explained that the water infrastructure utilizes several technical control systems to manage and track infrastructure properties, including hardware and software. Skiba further emphasized how these systems are more vulnerable to cyberattacks due to their complexity and internet connectivity (2020).

Zachary Lanz (2022), a recent SUNY Albany Cybersecurity program graduate, authored the article "Cybersecurity Risk in U.S. Critical Infrastructure: An Analysis of Publicly Available U.S. Government Alerts and Advisories." Lanz noted that the WWS is highly likely to fall victim to APTs. Furthermore, Lanz reported increased cyberattacks on critical infrastructures and the need for collaboration within the cybersecurity community. Typical TTPs utilized by APTs include ransomware, phishing, and denial of service attacks. These attacks could result in physical damage, service disruptions, or even death (2022).

Hugo Riggs, a machine learning and distribution system monitoring researcher, and his colleagues (2023) authored the article "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure." The authors also highlighted the increasing threats to critical infrastructures due to their integration with information technology. Riggs et al. predicted a significant increase in major cyber-attacks, highlighting their consequences, vulnerabilities, victims, and perpetrators, with costs reaching millions. Furthermore, the authors discussed innovative TTPs utilized to attack critical infrastructures and the consequences that followed (2023).

The *2023 Global Threat Roundup Report* by Vedere Labs provided a comprehensive analysis of cyber threats observed yearly (2023). Vedere Labs, the cybersecurity research branch of Forescout, reported current trends in cybersecurity, such as China's increase in originating attacks and web applications being the most frequently attacked service type. In addition, the report noted that APTs predominantly hailed from China, Russia, and Iran, targeting mainly the U.S., the United Kingdom, and Germany. The findings published in the report indicated that threat actors are focusing their efforts on targeting their efforts on targeting the infrastructure sectors, including power, water, industrial automation, and building automation (2023).

The Joint Cybersecurity Advisory (2021) consists of the Federal Bureau of Investigation (FBI), CISA, the Environmental Protection Agency (EPA), and the National Security Agency (NSA). This agency published the *Ongoing Cyber Threats to U.S. Water and Wastewater Systems* online advisory (2021). According to the joint advisory, additional TTPs utilized to compromise the U.S. WWS include spear-phishing, exploitation of internet-connected services and enabling remote access, exploitation of unsupported or outdated operating systems and software, exploitation of control system devices with vulnerable firmware versions, and utilization of insecure remote desktop protocol (RDP) connections to the internet (2021).

Juan Enrique Rubio has a Ph.D. in Computer Science from the University of Malaga. Rubio (2019) and others published the article "Current Cyber-Defense Trends in Industrial Control Systems" in *Computer and Security*, which provided an in-depth analysis of the cybersecurity threats to industrial control systems (ICS) with a focus on APTs. Rubio et al. highlighted additional cybersecurity threats that affect the industrial internet of things (IIoT) and cloud computing, which impact U.S. critical infrastructures (2019).

Dehghantanha Baharami is an academic cybersecurity and cyber threat intelligence entrepreneur. Baharami (2019) and others authored the article "Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures," which illustrated various ways threat actors deliver malicious payloads. For example, threat actors utilize email and social network spear phishing, website equipping, rogue software, removable media, and direct access to deliver payloads. Baharami et al. also emphasized the continuation of innovation by threat actors to execute payloads successfully and the need for proactive security measures (2019).

The Incident Response Guide: Water & Wastewater Sector (2024), published by the FBI, CISA, and EPA, outlined the importance and urgency of protecting the WWS by formulating an action plan and collaborating with various agencies. Collaboration allows for information sharing, collective analysis and response, resource optimization, coordinated messaging, enhanced cyber resilience, and minimizing risk to public health and safety and the economy. Since cyber incidents in the WWS are complex and have cascading effects, collaborating with others is more beneficial than focusing solely on TTPs (2024).

The WWS implemented several measures to mitigate cyber threats. Michal Shlapentokh-Rothman is a Ph.D. student at the University of Illinois. In the article "Coevolutionary Modeling of Cyber Attack Patterns and Mitigations Using Public Datasets," Shlapentokh-Rothman and colleagues (2021) described mitigating cyberattack patterns utilizing datasets. As they reported, utilizing datasets can assist with identifying which defensive actions are most effective, provide the necessary input to simulate realistic threat scenarios, rate the severity of vulnerabilities, and provide a historical context and trends necessary to analyze these dynamics. The development of

APTs in the cybersecurity landscape requires using datasets. APTs are a class of highly sophisticated cyberattacks perpetrated by groups of actors known for their TTPs (2021).

Maskie Malatji is a digital transformation and innovation academic at the University of South Africa. Malatji (2022) and others wrote the article "Cybersecurity Capabilities for Critical Infrastructure Resilience," which introduced the importance of cryptography as a means of mitigation and the challenges CIs face with the need for a robust cybersecurity framework as protection. Malatji et al. posited that cryptography can assist with data confidentiality, data integrity, authentication, non-repudiation, and secure communication. Further, cryptography protects from sophisticated cyberattacks such as man-in-the-middle attacks, eavesdropping, and data breaches (2022).

Colin Brooks is a senior IT Technical Analyst and Information Security Manager at Andar Software in New York City. Brooks (2019) wrote the article "Critical Infrastructure Protection at the Local Level," addressing the vulnerabilities and challenges of securing CIs, particularly water and wastewater treatment facilities, from cyber threats and threat actors. Brooks proposed employing frameworks like the National Institute of Standards and Technology (NIST), Risk Management Framework (RMF), the National Infrastructure Protection Plan RMF (NIPP-RMF), and the NIST Cybersecurity Framework for Critical Infrastructure to assess and mitigate risks effectively. However, Brooks reported that despite the availability of these resources, challenges persist in securing the WWS (2019).

As mentioned earlier, cyberattacks on any organization cost money. Mubarak Himmat is an assistant professor and Dean of the Faculty of Computer Science at Future University in Sudan. Himmat (2023) and others published the article "The Current Trends, Techniques, and Challenges of Cybersecurity," which discussed the impact of cyberattacks on different sectors

and national governments' development of cybersecurity strategies. The authors reported that the most powerful countries in cyberspace include the United Kingdom, the U.S., France, Lithuania, Estonia, Spain, Singapore, Norway, Malaysia, Canada, and Australia. The rise of cyberattacks has prompted national governments to reconsider their perception of cybersecurity risks and the potential impacts on society, the economy, and critical infrastructures (2023).

Humairaa Yacob Bhaiyat, a software developer, and Siphesihle Philezwini Sithungu, a Computer Science Ph.D. candidate specializing in Applied Artificial Intelligence (AI), wrote the article "Cyberwarfare and its Effects on Critical Infrastructure" (2022), which explained the effects of cyberwarfare on critical infrastructures and human life. The authors recognized the economic impact of cyber warfare and the necessity for mitigation. They discussed various strategies, such as improving network security, implementing robust incident response plans, and promoting international cooperation in cybersecurity. These measures are crucial as economic losses from cyber warfare can lead to the loss of human life (2022).

David Lloyd Owen, an international business executive and director of cybersecurity and intelligence based in West Wales (2021), wrote the article "Cybercrime, Cybersecurity, and Water Utilities," which focused on increasing cybercrime incidents affecting water utilities. According to Owens, cybercrimes have had a tangible and detrimental effect on countries' economies. Past cyberattacks have cost millions of dollars in damages, and these costs can have a significant impact on the financial stability of water utilities. Cyberattacks can affect the overall economy by increasing operational expenses and potentially leading to service disruptions. As Owen noted, water utilities also face significant forms of cybercrime, including extortion by organized crime groups, corporate theft, and other acts of terrorism perpetrated by

state actors such as China, Iran, and Russia to damage public trust and confidence in the governments and utilities of the target countries (2021).

Christine Li (2022), a professor at the City College of New York (CUNY), wrote the article "Securing U.S. Critical Infrastructures Against Cyberattacks," which addressed the pressing issue of securing U.S. critical infrastructures from cyberattacks and emphasized the urgency following the cyberattack on the Colonial Pipeline by the DarkSide hacker group. This attack disrupted nearly half of the Eastern Seaboard's fuel supply and highlighted the nation's vulnerability and private ownership of most U.S. critical infrastructure. Li estimated that cyberattacks will cost the U.S. economy approximately $10.5 trillion annually by 2025 (2022).

The general problem is that cyberattacks targeting critical infrastructures, such as water and wastewater, pose a growing threat to the nation's security, public health, and economic vitality (Brooks, 2019; CISA, n.d.; Riggs et al., 2023). Despite their importance in sustaining modern life and economic activity, the 16 critical infrastructures are increasingly vulnerable to sophisticated cyber threats posed by adversaries such as APTs. Critical water infrastructure systems are at risk because APTs use TTPs to exploit vulnerabilities. APT groups are persistent, underscoring the need for a comprehensive understanding of the TTPs used by these groups, their motivations, and the development of effective mitigation and defense strategies for protecting these critical infrastructures.

The specific problem is current TTPs utilized by APTs to target critical infrastructures in the U.S. maliciously, specifically the WWS, for various motives such as espionage, sabotage, intimidation, theft of operational data, terrorism, and economic disruption (Lanz, 2022; Owen, 2021; Rubio et al., 2019). Current TTPs allow threat actors to compromise information and operational technology networks, systems, and devices. Understanding TTPs is crucial because

they characterize the behavior of threat actors in terms of how they orchestrate and manage their attacks. Therefore, it is essential to understand and study TTPs utilized by APTs as this knowledge will assist with protecting CIs for national security, public health, and economic stability.

Literature Review

This paper includes various reputable academic journals, scholarly articles, and industry reports to ensure accuracy and credibility. Authors such as Zachary A. Lanz (2022), Tobi A. and West, Aeron Zentner (2019), Amin Hasanzadeh et al., and Amit Sharma et al. (2023) were reliable resources whose expertise significantly contributed to this work. Furthermore, a comprehensive overview of the subject included synthesizing complex concepts, exploring various perspectives, and analyzing data to present a well-informed and evidenced-based narrative. This paper draws upon several reputable academic journals, scholarly articles, and industry reports to provide a strong foundation for understanding the importance of analyzing current TTPs employed by APT groups in targeting critical infrastructures.

Learning From TTPs Employed by APT Groups Targeting Critical Infrastructures

Previous Cyberattacks on the United States' Critical Infrastructures

Tobi West, the department chair of the Computer Information Systems and Cybersecurity at Coastline College, and Aeron Zentner, the Dean of Institutional Effectiveness at Coastline College, wrote the article "Managing Security Risks: An Assessment of U.S. Critical Cyber Infrastructure Protection" (2023). West and Zentner reported that the U.S. has experienced a significant increase in cyber incidents targeting critical infrastructures; federal agencies reported an increase of 1300% from 2006 to 2015. In addition, Verizon's *Data Breach Investigations Report* (2023) revealed that 16% of the 2013 confirmed data breaches in 2019 were public sector

entities, indicating a significant impact on critical infrastructures. The report also highlighted a dramatic increase in attacks executed by nation-state actors, increasing from 12% in 2018 to 23% in 2019. These aforementioned incidents underscore the escalating cyber threats faced by the United States' critical infrastructures (2023).

Amin Hasanzadeh is a visiting associate professor at Pennsylvania State University's Smeal College of Business and has served as a faculty member at the National University of Iran's Department of Actuarial Science. Amin Hasanzadeh (2020) and others published the article "A Review of Cybersecurity Incidents in the Water Sector," which discussed cyberattacks and the WWS. In 2020, the Rye Brook, New York Water Utility experienced a ransomware attack. Specifically, the attack involved data encryption, leading to operational disruptions. The attackers demanded a ransom to restore access; however, the utility declined to pay, as they could unlock the data. Despite multiple layers of protection, the utilities IT system was still penetrable, yielding to the growing threat of ransomware attacks (2020).

Lanier Watkins has a doctorate in Philosophy of Computer Science and is currently the Senior Cyber Research Scientist at Johns Hopkins University. Watkins and colleagues (2022) wrote the paper *Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack* and expanded on the cyberattack on the Oldsmar Water Treatment Facility in Florida that occurred on February 5, 2021. The threat actor accessed the plant's operator console using compromised credentials and TeamViewer's remote access software. Then, the threat actor increased the sodium hydroxide in the water supply to dangerous levels, posing a significant health risk to thousands of people supplied by the plant. The system operator identified and corrected the attack, reducing the overall impact (2022).

Robert Grubbs is based in Arlington, Virginia, and is a Senior Cyber Intelligence Analyst at Idaho National Laboratory. Grubbs et al. (2022) wrote the paper *Evolution and Trends of Industrial Control System Cyber Incidents Since 2017.* They discussed how Ellsworth County, Kansas's Post Rock Water District, experienced a cyberattack. According to the report, Wyatt Travnichek, a former employee, allegedly attempted to alter the disinfectant levels by logging into the computer system, as his credentials were still accessible. On March 27, 2019, Travnichek could access the system remotely using his cellular phone and shut down the plant. In addition, once in the system, Travnichek shut down the plant and turned off one filter. This incident highlights the vulnerability of both information and operational technology and underscores the necessity for robust operational security practices. Moreover, this incident emphasized the significance of resiliency testing for assets deployed within the operational and information technology environments (2022).

Grubbs and colleagues (2022) also reported another cyberattack regarding the Knoxville, Tennessee, water and wastewater treatment plant. The City of Knoxville experienced a ransomware attack in 2020, which targeted city websites and caused delays with several city services. The threat actors contacted the city via a message on a compromised server in early May. Although the town reported preparedness with the detection systems, the threat actors deployed ransomware one weekend when the IT office had fewer on-site employees. The attack negatively affected the ability to obtain police reports, pay utility bills, and connect new utilities, such as water; new residents reported being without water for days following the service request. The city's chief information officer estimated that approximately 40% of its servers and 20% of its laptop and desktop computers were damaged or encrypted. This attack resulted in the release of roughly 18,000 exfiltrated files (2022).

Scott Buchanan, a doctorate student of Science in Cybersecurity at Capitol Technology University, authored the paper *Cyber-Attacks to Industrial Control Systems Since Stuxnet: A Systematic Review* (2022). Buchanan reported a cyberattack on the San Francisco Area Water Facility in January 2021. The threat actor used stolen credentials on an outdated operating system and TeamViewer, a desktop-sharing application. An operator watching the facility's industrial control system human-machine interface identified the cyberattack. Buchanan noted that these aforementioned incidents underscored the vulnerability of critical infrastructures to cyberattacks and the importance of securing operational and information technology systems (2022).

Muhammad Muzammil Aslam is a Ph.D. student from Pakistan with a master's in information and communication engineering from USTB Beijing, P.R. China. Aslam et al. (2023) wrote "A Comprehensive Study on Cyber Attacks in Communication Networks in Water Purification and Distribution Plants: Challenges, Vulnerabilities, and Future Prospects" and described the Rivera Beach Water Utility attack. According to the authors, the attack on the Rivera Beach Water Utility occurred on May 29, 2019. A police department employee opened ransomware that affected several entitlements, such as government offices and the water utility. The attack compromised the computer systems responsible for water quality testing and payment handling. Unfortunately, the city council agreed to pay the threat actors 65 bitcoins, equivalent to $600,000.00. In addition, the city had to allocate an additional $25,000.00 from its budget to cover insurance deductibles. The city invested an additional $900,000.00 in new hardware and computers as the older equipment was outdated and vulnerable. The FBI, Secret Service, and the Department of Homeland Security (DHS) investigated the incident and advised against paying

the ransom. This attack focused on the vulnerability of small towns and cities to threat actors and outdated systems (2023).

Advanced Persistent Threats (APTs)

Amit Sharma is the CEO of CData Software in Chapel Hill, North Carolina. Sharma (2023) and others wrote the article "Advanced Persistent Threats (APT): evolution, anatomy, attribution, and countermeasures" and described APTs as highly sophisticated and targeted cyberattacks with specific objectives, intricate attack vectors, and advanced malware. APT attacks are stealthy and evasive, making them difficult to detect. Such attacks can involve zero-day and negative-day exploits and payloads executed by well-funded threat actors such as nation-states or corporate entities. The article mentioned well-resourced groups, including APT-41 Double Dragon Group, Ke3chang, APT-1 Common Crew, Black Oasis, and the Sandworm Team (2023). These APT groups are known for their sophisticated and targeted attacks with specific objectives. The objective of APT attacks is to compromise organizations' survivability, availability, confidentiality, and integrity, and the development and maintenance of such attacks generally require significant resources and time. Developing better defense systems requires understanding the internal components of these attacks. Moreover, it is vital to understand how APT attacks operate to develop effective defense mechanisms to mitigate their on digital infrastructure (2023).

Techniques, Tactics, and Procedures

Martti Lehto is a working professor of cybersecurity at the University of Jyvaskyla and a retired military colonel, and Pekka Neittaanmaki, a professor of Scientific Computing and Dean at the University of Jyvaskyla edited "Cyber Security Critical Infrastructure Protection." Lehto and Neittaanmaki (2021) reported that APTs employ a variety of TTPs to achieve their

objectives, typically espionage, data theft, or system disruption. The most popular TTPs used by APTs, as distilled from the provided context, include spear-phishing, water hole attacks, and exploiting vulnerabilities. Spear-phishing includes utilizing highly targeted emails with malicious attachments to gain initial access. Water hole attacks compromise commonly visited websites to infect a targeted organization's systems. Exploiting vulnerabilities is when threat actors utilize known or zero-day vulnerabilities to gain access to systems. Additional TTPs used by APTs include escalating privileges, moving laterally, using command and control servers, using backdoors, polymorphism and metamorphism, timing-based evasion, environment checks, secure shell tunnels, manipulating network protocols, malware, DDoS attacks, targeting third-party vendors, phishing, exploiting human error, advances malware variants, and customized attack tools (2021).

TTPs and Critical Infrastructures

There have been incidents of TTP attacks on critical infrastructures, as reported by Lehto and Neittaanmaki (2021); for instance, targeted spear phishing attacks to gain network access, as evidenced by Korea Hydro and Nuclear Power. Malicious malware like Shamoon, BlackEnergy, and Petya disrupt services or wipe data, targeting companies like Aramco and the Ukrainian power grid. DDoS attacks overloaded systems with traffic to disrupt services such as heating distribution. False data injection attacks disrupted the operations of smart grids. Exploiting trusted relationships focuses on an industrial control system to deliver payloads effectively. Lastly, adversarial attacks involve deceiving machine learning models, such as those controlling HVAC systems in smart buildings, to cause security breaches or spikes in energy consumption. Threat actors use these TTPs as a sophisticated arsenal for compromising and potentially damaging critical infrastructure. The diverse nature of TTP attacks on critical infrastructures

highlights the urgent need for robust cybersecurity measures and proactive defense strategies to combat evolving threats (2021).

Importance of the Water and Wastewater Infrastructure on Health and the Economy

Apurva Pamidimukkala is an Assistant Research Professor at the University of Texas at Arlington Department of Civil Engineering. Pamidimukkala et al. (2021) wrote the article "Resilience in Water Infrastructures: A Review of Challenges and Adoption Strategies," which identified the importance of this critical infrastructure. WWS's importance is multifaceted and, if compromised, can be cataclysmic. The WWS ensures safe and clean water for the healthy functioning of society. Furthermore, WWS protects the environment from pollution, as this sector manages wastewater collection, treatment, and disposal. Also, the WWS contributes to economic growth by providing employment opportunities and supporting other industries that rely on water as a resource. The WWS supports social well-being, as access to water enhances the quality of life and supports various activities such as recreation. Additionally, the WWS plays an essential role in disaster response and recovery. A resilient water and wastewater infrastructure will ensure uninterrupted access to water services during and after natural disasters. WWS must adapt and expand to meet the needs of a growing population and ensure that future generations have access to clean water and sanitation services (2021).

Impact on Economic Activities and Industries

Pamidimukkala et al. (2021) discussed the ripple effect in the economic structure when the WWS is compromised. For instance, any damage, such as cyberattacks, is expensive, and repair and replacement costs burden public and private financial resources. Businesses that rely on water for their agriculture, manufacturing, and tourism operations can experience disruptions. These disruptions can lead to reduced productivity, revenue, and job losses. Waterborne diseases

can increase healthcare costs and pressure the healthcare system. There is a risk that a lack of confidence in the quality of water services may discourage investment in affected areas, leading to a reduction in economic growth. Moreover, areas with unreliable water and wastewater services can deter investment in affected regions, slowing economic growth and development. Slowing economic development can negatively impact property values, affecting wealth and tax revenues. The economic impact of a compromise on water services may also worsen socioeconomic disparities (2021).

Pitor Lis is the Deputy Head of the School of Economics, Finance, and Accounting at Coventry University, and Jacob Mendel is a cybersecurity and blockchain expert, and the Executive Director of Applied Research at JPMorgan Chase & Co. Lis and Mendel (2019) wrote the article "Cyberattacks in Critical Infrastructure: an Economic Perspective," which reported several additional indirect economic effects from an attack on the WWS. Specific examples include disruptions to supply chains and economic activity. An attack on the WWS can disrupt supply chains that depend on water as a critical input. A disruption can ripple through the economy, affecting various industries and potentially slowing economic activity. Disruptions and potential shutdowns of local businesses can decrease tax revenue for local and national governments, and both entities rely on business operations for tax income. Increased cybersecurity threats may enhance government policies, which will lead to an increase in regulatory compliance costs. End users such as taxpayers or consumers absorb these costs. Additional insurance costs from perceived cyberattacks in the WWS can increase insurance premiums for businesses and others within related sectors. Also, cyberattacks can negatively affect or deter foreign investors from investing in regions or countries affected by an attack. The trust in the WWS can erode, leading to long-term reputational damage that may affect economic

relationships and market positioning. Customer relationships and contracts may negatively affect businesses relying on the WWS. Reduced customer relations and severed contracts are possible if businesses cannot deliver services or products secondary to disruptions (2019).

Lis and Mendel (2019) mentioned the 2018 Onslow Water and Sewer Authority (ONWASA) cyberattack in North Carolina. A ransomware attack known as Ryuk, using Emotet, a sophisticated banking Trojan, spread throughout the water department's network, leading to the encryption of databases and files. The water utility did not pay the ransom for the decryption key. However, the attack resulted in an economic disruption. Significant costs were associated with the system's recovery and data loss and the potential impact on water services critical to various economies following the attack. Several utilities and government agencies have increased their cyber defenses to prepare for future attacks following strong recommendations. The integrity and resilience of the WWS are vital for public health and environmental protection and sustaining economic stability. Therefore, protecting systems that assist critical infrastructures, such as ICS, is imperative (2019).

Industrial Control Systems

Thomas Miller is a Ph.D. student at Lancaster University in the United Kingdom. Miller and others (2021) wrote the article "Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems," which detailed extensive cyberattacks on industrial control systems (ICS). Miller et al. (2021) described ICS as a combination of software and hardware working together to control and manage industrial processes. ICS are essential for the operation of various processes and are essential for the operation of various complex industrial environments such as the Critical National Infrastructure (CNI). ICSs usually consist of components that fall into distinct zones or levels, such as the safety zone, the manufacturing

zone, the demilitarized zone, and the enterprise zone. ICSs have continually evolved with the complexity and connectivity of technology, and their interconnectivity presents new vulnerabilities and cybersecurity challenges. Threat actors exploit vulnerabilities to cause operational shutdowns, financial loss, equipment damage, and the potential loss of human life (2021).

Cyberattacks on ICS

Miller et al. (2021) reported on the evolution of cyberattacks on ICS from the 1980s to 2021. The authors noted key trends in cyber threats, including a shift from individual threat actors to organized groups and a change in attack motives from personal to political reasons following 2009. As technology progressed and ICS became more interconnected, the attack real estate expanded, with threat actors leveraging standard protocols and social engineering for access. In order to maximize impact, threat actors targeted sectors with interdependencies such as WWS. Therefore, the importance of cybersecurity has grown since the discovery of Stuxnet in 2010 and SolarWinds in 2019, highlighting the potential damage of such attacks on critical infrastructures (2021).

The Critical Role of Information Technology Systems & Protecting Critical Infrastructures

Maurice Dawson Jr., Ph.D., is the Cyber Security Center Director at the Illinois Institute of Technology. Dawson and others (2021) wrote the article "Understanding The Challenge of Cybersecurity In Critical Infrastructure Sectors," which discussed the vital concern for protecting 16 critical infrastructures in the U.S. secondary to their impact on national security, public health, and the economy. Dawson et al. (2021) highlighted the integral role of information technology (IT) systems in supporting critical infrastructures. IT systems are essential for these infrastructures' control, communication, and operations, enabling operational control through

Supervisory Control and Data Acquisition (SCADA) systems. Furthermore, IT is also vital for ensuring security and resilience against cyber threats while complying with cyber security standards and regulations. Overall, protecting IT systems is critical for maintaining national security and the functionality of critical infrastructures (2021).

Effect on Health & Well-Being

Umit Cali is a University of York professor specializing in Advanced Data Analytics. Cali and others (2023) wrote the article "Cyber-physical Hardening of the Digital Water Infrastructure," which discussed the challenges and solutions for protecting digital water infrastructure against cyber-physical threats. Also, the authors mentioned the importance of the water infrastructure to health and well-being; WWS is a fundamental service essential for sustaining life and maintaining public health. The WWS ensures the delivery of clean and safe water for drinking, cooking, and hygiene, which are necessary for preventing disease and promoting health. Furthermore, these systems are responsible for removing wastewater and preventing contamination of water sources and the environment (2021).

Watkins et al. (2022) provided an example of a cyberattack on a WWS and its adverse effects on public health and well-being. As mentioned, Florida's Oldsmar Water Treatment Facility sustained a cyberattack in February of 2021. The threat actor attempted to increase the levels of sodium hydroxide in the water supply from 100 parts per million (ppm) to 11,000 ppm, which is over 100 times the intended amount. Direct exposure to sodium hydroxide can cause painful burns. Also, ingestion of sodium hydroxide can cause permanent internal damage. Oldsmar's systems operator detected the malicious activity, corrected the chemical levels, and minimized the impact. However, if the attack were not detected and mitigated, the elevation of sodium hydroxide would reach thousands of people and expose them to dangerous water (2022).

Tejasvi Alladi is an assistant professor at the Department of Computer Science and Information Systems at BITS-Pilani. Alladi and others (2020) wrote the article "Industrial Control Systems: Cyberattack trends and countermeasures," which discussed cybersecurity threats faced by ICS, specifically the ICS at the Kemuri Water Company. The Kemuri Water sustained a cyberattack in 2015 with potentially serious implications. A Syrian hacktivist group was a prime suspect, but the intentions behind the attack were unknown. In addition, the attackers exposed the personal data of 2.5 million customers, and compromised the outdated IBM AS/400-based SCADA system, which managed the Programmable Logic Controllers (PLCs) (2020).

These PLCs were responsible for regulating the flow of water and chemicals by controlling valves and ducts within the plant (Alladi et al., 2020). The attack occurred twice, and the threat actors successfully altered the quantity of chemicals used in water treatment via the PLCs web interface. This action disrupted the plant's production and increased the time required to replenish water supplies. There was no reported impact on the plant's operations, regardless of manipulating the plant's chemical control valves. The Syrian hacktivist group lacked a deeper understanding of SCADA systems; however, the surrounding communities and the plant could have sustained severe consequences, such as harm to individuals' health. Therefore, based on this information, critical infrastructures need a better understanding of APT groups and implementing mitigating strategies to create an aggressive defensive system (2020).

Understanding Threat Actors, Attacks, and Defensive Measures

APT Groups Main Objectives

Martti Lehto (2022) described that the main objective for APT groups is to maintain ongoing access to the targeted network and obtain data. These objectives are those of nation-

states or state-sponsored groups; the stolen data can include intellectual property, business contracts, negotiations, secret policy, military papers, and other sensitive information. The goal is to obtain such information for political, military, or financial gain. APT attacks, characterized by their stealth and sophistication, target high-value entities to extract valuable secret information. Furthermore, APT attacks may involve the manipulation of data, which is considered one of the most dangerous forms of cyberattacks, secondary to its ability to corrupt or overwrite valuable data (2022).

Challenges Detecting APT

Sharma (2023) discussed the various challenges organizations face in detecting APT attacks secondary to their complexity and sophistication. For example, challenges such as the complexity of attack vectors pose a significant threat to targeted victims. The malware is stealthier and more evasive, while zero-day and negative-day exploits are becoming more common. In addition, APTs are utilizing TTPs, which makes it more difficult to attribute responsibility and conceal their identity. The malware is more precise and capable of evading detection by target defenses, as many organizations are poorly equipped with the technology appropriate to counter APT attacks effectively and efficiently. Analyzing large volumes of network traffic and logs is resource-intensive and requires advanced analytical tools. Additional limitations include sharing threat intelligence and limitations within the available data. Open-source intelligence (OSINT) plays a vital role in analyzing APT attacks. Lastly, APTs are often politically or economically motivated, which involves understanding the adversary's strategic goals. The lack of understanding of goals and objectives makes identifying APTs difficult (2023).

Cyberattack Phases

APT cyberattacks are executed in several distinct phases, as explained by Lehto (2022). A lifecycle approach describes the sophistication and execution of cyberattacks. The variety of APT attacks has led to the development of several models, such as MITRE ATT&CK, Mandiant Attack Lifecycle Model, LM Cyber Kill Chain, Unified Kill Chain, and Hybrid Cyber Kill Chain. However, Lehto (2022) described the general APT cyber-attack model and divided a cyberattack into several distinct phases. The first phase is the early-attack phase, which involves strategic decision-making, where the attacker makes strategic decisions regarding the target and the objectives of the overall attack. The pre-attack phase includes reconnaissance activities such as location, target identification, and characteristics. In addition, this phase involves weaponization, where threat actors develop malware that coincides with the vulnerabilities identified during the reconnaissance phase. Next, the attack phase, segmented into smaller subsections, is executed in the following order: penetration, persistence, exploitation, installation, evasion, lateral movement, command and control, and execution. The end state is the last phase and signifies the completion of the objectives; the threat actor attempts to leave without notice by not leaving any traces of their presence in the information and communication technology system. However, if the threat actors successfully extract data undetected, they might remain inside the network for future opportunities and create backdoors, known as hidden methods of bypassing standard authentication or encryption in a computer system, for re-entry (2022).

APT Groups Target U.S. Critical Infrastructures

Sharma (2023) explained how APT groups target the U.S. critical infrastructures. As mentioned previously, cyberattacks utilize sophistication and targeted cyberattack strategies.

APT groups are well-resourced, organized, and often supported by nation-states that employ intricate attack vectors to achieve their objectives. APT groups utilized several methods to target critical infrastructures. The most utilized method is spear phishing, in which threat actors send emails with "weaponized" attachments or links. The information gathered during the reconnaissance stage allows APT groups to manipulate recipients into opening emails and accidentally installing malware. Watering hole attacks occur when APT groups compromise websites frequently visited by employees of critical infrastructure entities. These websites have embedded payloads and can selectively infect visitors based on factors such as IP addresses, delivering malware to the intended targets. Zero-day vulnerabilities allow APT groups to infiltrate systems and networks when no patches are available to detect and stop such threats (2023).

As demonstrated during Stuxnet, removable media such as USB devices infected with malware are often used in air-gapped systems (Sharma, 2023). APT groups often use custom malware to focus on the defenses and systems of the target infrastructure. Command and control (C2) servers are also used by APT groups because, once inside a network, they can exfiltrate sensitive data, manipulate systems, and obtain their objectives discretely. Social engineering tactics are popular with APT groups as they allow threat actors to manipulate victims by providing information that assists in compromising critical infrastructure systems. Exploiting publicly known vulnerabilities occurs when APT groups monitor hacker communities and public disclosures for known vulnerabilities and rapidly incorporate them into their attack strategies before system patches are available. APT groups have also used system patches to spread malware and break into organizations' networks (2023).

SolarWinds Attack

Rahaf Alkhaldi is a software engineering student at Prince Mohammad Bin Fahd University. Alkhadra and others (2021) wrote the article "Solar Winds Hack: In-Depth Analysis and Countermeasures" and thoroughly explained the SolarWinds attack. The SolarWinds attack was a significant attack that compromised several private and public organizations. Although the SolarWinds did not attack physical critical infrastructures like power grids and water systems, it attacked the supporting government agencies. SolarWinds affected several U.S. federal agencies, such as the Department of Commerce, Department of Defense (DoD), Department of Energy (DOE), National Institutes of Health, Department of the Treasury, and the Department of State. Russia's Foreign Intelligence Service was the prime suspect in the SolarWinds attack (2021).

Alkhadra et al. (2021) explained how the threat actors executed the SolarWinds breach by inserting malware into a software update from the SolarWinds Orion software. The malware was distributed to SolarWinds clients when they installed the compromised update, as the malware created a backdoor that allowed threat actors to access the more extensive system of SolarWinds' clients. FireEye, a cybersecurity company, discovered the attack and revealed that the threat actors utilized techniques to avoid detection by security tools and remain incognito within networks. The breach affected approximately 18,000 SolarWinds clients, including supportive federal agencies and critical infrastructures (2021).

Implementation and Understanding of Effective Defense Strategies

David Lloyd Owen (2021) explained the importance of understanding and implementing effective defense strategies for protecting against cyber threats that target water and wastewater facilities as cyberattack threats, severity, and frequency have increased. As mentioned in the former, SCADA systems are utilized in WWS to monitor and control infrastructure processes. It

is important to note that facilities are vulnerable to exploitation without adequate staff education regarding phishing attacks and implementing cybersecurity measures. Nation-states, irked employees or former employees, and organized crime groups are constantly targeting WWS, which places the public at risk (2021).

Cyber threats constantly evolve, and critical infrastructures are targeted worldwide (Owen, 2021). Threat actors utilize technological advancements to make their attacks more sophisticated, efficient, and complex to detect. Potential gains such as monetary gain, information gathering, or causing physical harm influence cybercrimes. For example, Russia has targeted the WWS in the U.S., intending to damage public trust and confidence in the utilities within the targeted country. Owen reported that the cost associated with cybercrime is more expensive than investing in cybersecurity. Therefore, it is in the WWS' best interest to invest in cybersecurity to protect overall operations and customer data (2021).

Dr. Sridar Adepu is a Cyber-Physical Systems Security in Computer Science lecturer at the University of Bristol. Adepu and others (2019) wrote the article "Investigation of Cyber Attacks on a Water Distribution System," which focuses on the impact of cyberattacks on the WWS and the design of an attack detection mechanism. In addition, the authors agreed that understanding and proactively establishing cybersecurity defense strategies is imperative for safeguarding critical infrastructures such as the WWS. Cyberattacks can negatively impact water distribution systems, including tank overflows, pressure drops, damage to equipment, and disruption of water distribution to consumers. Understanding a waste distribution system's response time to a cyberattack allows cybersecurity specialists to design an effective and efficient attack detection mechanism. Knowledge of time and response allows for the development of robust defense strategies that can detect and mitigate cyberattacks and reinforce

the safety and security of water distribution, as targeted cyberattacks have become more advanced as APTs have utilized advancements in technology and become more aggressive with attacks (2019).

Jim McCarthy (2023) is a senior security engineer at the National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence and authored the paper *Cybersecurity For The Water And Wastewater Sector,* and reported that cyberattacks are aggressively becoming more innovative secondary to the increasing adoption of network-enabled technologies in critical infrastructures such as the WWS. As automation, sensors, data collection, and network devices become more integrated, vulnerabilities continue to increase. In addition, McCarthy et al., noted that the conglomeration of operational technology with information technology invited new entry points for malicious threat actors to exploit. This conglomeration is copacetic with Miller (2021), who noted that the attack platform expanded as technology progressed and ICS became more interconnected. McCarthy also reported that threat actors utilize credential harvesting, phishing campaigns, and man-in-the-middle attacks to gain unauthorized access to networks and compromise data integrity. The need for sector-wide improvements in cybersecurity to address these evolving threats is imperative (2023).

Discussion of the Findings

The purpose of this research was to analyze tactics, techniques, and procedures (TTPs) utilized by Advanced Persistent Threat (APT) groups to target United States (U.S.) critical infrastructures (CIs) and provide insights into mitigations and defense strategies. Why is it essential to analyze current TTPs employed by APT groups for targeting critical infrastructures? Why is protecting U.S. critical infrastructures like Water and Wastewater necessary for our nation's safety, public health, and economic vitality? How do APT groups target the United

States' critical infrastructures, and why is understanding and implementing effective defense strategies essential for deflecting these threats?

Learning From TTP Employed by APT Groups Targeting Critical Infrastructures

Motives of APT Groups and WWS

Tobi West and Aeron Zenter reported that motives and strategic objectives vary depending on key factors, such as the nation-states and organized groups endorsing the cyberattack. However, the main objective of APT groups is to maintain access to targeted networks, retrieve valuable data such as intellectual property, compromise an organization's integrity, and display its overall vulnerability. The APT groups, such as Conti, are often supported by well-resourced, funded, and organized nation-states. However, ransomware attacks are the most common in many cases reviewed within this paper. A threat actor or APT group would often demand payment to restore access to compromised systems. The compromised systems could yield catastrophic results, such as turning off water treatment plants' filters, altering the water's chemical composition and water testing, payment and handling, or shutting off water delivery to consumers entirely. Often, cryptocurrency, such as Bitcoin, is requested as a payment to restore or correct water services. The overall objective of attacking WWS is to disrupt the functioning and compromise public health, safety, and national security. Threat actors and APT groups intend to cause significant economic and social disruption, create chaos, undermine public confidence, and potentially gain leverage for political or financial gain.

Common Trends in Attacks on WWS

Several characteristics of how threat actors conducted cyberattacks on WWS were discovered throughout the research, as evidenced by Cervini et al. and Buchanan. The first common characteristic was using compromised credentials to access software, as evidenced

during the Oldsmar water treatment plant. Once the threat actor obtained access to the TeamViewer software, they could control and execute specific commands and manipulate the chemical composition, placing many at risk. Furthermore, significant economic fallout followed the attack, as the Super Bowl was scheduled within this affected region, negatively affecting many fans' ability to attend the game.

The San Francisco Bay Area Water Facility attack was similar to the Oldsmar attack, as Buchanan reported in his article. A hacker used stolen credentials to access the water treatment facility's operating system. Once inside the outdated operating system, the threat actor could utilize the same TeamViewer software identified in the Oldsmar attack. This tactic allowed the user to change the water's chemical composition from a remote location, which could cause existential damage to consumers' health. In both cases, threat actors could obtain compromised credentials, access the ICS human-machine interface, and use the TeamViewer software to augment chemicals within the water treatment process. Unfortunately, neither Cervini et al. nor Buchanan could provide information about the responsibility for either attack. Cervini et al. reported that an unknown individual or group gained access to Oldsmar's water facility, as Buchanan suggested the possibility of Russia being responsible for the San Francisco attack; however, no definitive party was held responsible in either paper.

The Oldsmar and San Francisco water facilities were not the only cases that shared similar cyberattacks. Rivera Beach Water Utility and the City of Knoxville were both subject to Ransomware attacks. A police department employee in Rivera Beach opened ransomware from an infected email, which spread to other city coworkers. Of course, this malware spread to government offices and the water utility department, encrypting data. The computer systems control the pumping stations, water purity testing, and handling payments for such services.

Threat actors also deployed ransomware in the City of Knoxville attack. However, Grubbs and others did not explain important information within their article, such as how the attackers installed the ransomware on the city's networks. Simply, the ransomware was installed, which disrupted services such as the ability to obtain police reports, pay utility bills, and allow consumers to access water. The authors did not identify the specific well-known TTPs used in the attack but did mention Conti as the group responsible for the attack.

The Rye Brook Water Utility, as reported by Hasanzadeh et al. and others, was a more recent attack in 2020. The authors explained how threat actors used ransomware cyberattacks against the Rye Brook Water Utility and encrypted data. Like the Rivera Beach Water Utility, the attackers demanded a monetary reward attack in order to restore access. Although the article provided detained information regarding various cybersecurity incidents and the WWS, some information was missing. For instance, Hasanzadeh et al. did not present a comprehensive analysis of the ramifications of cyberattacks on WWS regarding financial and operational impacts. Also, the article did not address specific mitigations and best practices that would be advantageous for protection. Finally, the authors failed to mention who was responsible for the attack but said they were state-sponsored. Knowing who committed the cyberattack will significantly improve proactive defensive cybersecurity strategies.

Common APTs

Sharma et al. reported on the various APTs, labeling them highly sophisticated, evasive, and challenging to detect; nation-states often endorse them. Owen revealed that China, Russia, and Iran are the most common nation-states that endorse APTs. These nation-state-funded APTs, threat actors, and terrorists execute cyberattacks on WWS. More specifically, Sharma described APT-41 Double Dragon Group, Ke3chang, APT-1 Common Crew, Black Oasis, and the

Sandworm Team as sophisticated, well-resourced, and stealthy. Understanding how the APTs operate, their objectives, motives, and primary funding sources is imperative, as this information will allow critical infrastructures to better protect and defend from cyberattacks.

TTPs and Critical Infrastructures

Research by Lehto and Neittaanmaki's article described the TTPs used by threat actors, such as spear phishing attacks to gain network access, malware to disrupt services or wipe data, and DDoS attacks used to overload systems with traffic to disrupt services. The most popular TTPs used by APTs, as distilled from the provided context, include spear phishing, waterhole attacks, and exploiting vulnerabilities. Lehto and Neittaanmaki further explained how TTPs assisted attacks when targeting victims' networks and operating systems. Although the article provided examples of popular TTPs utilized during cyberattacks against critical infrastructures, such as Korea Hydro and Nuclear Power and Aramco and the Ukrainian power grid, a more in-depth comprehensive analysis of specific details regarding the TTPs would support the cases mentioned within the article.

Lehto and Neittaanmaki provided an analysis of the impact of digitalization on society and current TTPs used when targeting critical infrastructures such as the WWS. For example, they explained how spear phishing allowed threat actors to gain network access, as evidenced by the previously mentioned Korea Hydro and Nuclear Power attacks. The authors also cited malware like Shamoon, BlackEnergy, and Petya that disrupted services and wiped or corrupted data. Spear phishing and malware are often used in cyberattacks, as evidenced in the Rye Brook Utility, City of Knoxville, and Rivera Beach water utilities. Although spear phishing and malware are often used in cyberattacks, any useful TTP is possible if successfully used to execute a cyberattack by a threat actor or an APT group.

Why is protecting U.S. critical infrastructures like Water and Wastewater necessary for our nation's safety, public health, and economic vitality?

Water and Wastewater Critical Infrastructure

The CISA reported that the WWS is one of 16 critical infrastructures in the U.S. and that all 16 are vulnerable to cyberattacks. The CISA also reported that approximately 153,000 public drinking water and 16,000 public wastewater treatment plants exist within the U.S. The WWS upholds the economy and the overall health of the general public. Richard Skiba highlighted the need for cybersecurity and the protection of U.S. critical infrastructures as the number of cyberattacks targeting WWS continues to increase. Also, Skiba brought attention to the vulnerability of the technical control systems, including the hardware and software that enable the WWS function. Moreover, Skiba noted that as the advancement in technology increases, so will the vulnerability of the WWS operating systems.

Lanz concurred with Skiba regarding cyberattacks and the WWS and reported that the WWS is highly likely to fall victim to APTs; he highlighted the increase of cyberattacks on critical infrastructures and the need for collaboration within the cybersecurity community. Like Lehto and Leittaanmaki, Lanz reported phishing as a popular TTP; however, Lanz noted that ransomware and denial of service attacks often cause physical damage, service disruptions, or even death. Riggs and others agreed with Lanz, Lehto, and Neittaanmaki regarding cyberattacks on critical infrastructures. Riggs et al. predicted a significant increase in major cyber-attacks, highlighting their consequences, vulnerabilities, victims, and perpetrators, with costs reaching millions. Moreover, Riggs and colleagues indicated that the TTPs used to attack critical infrastructures such as the WWS have become more innovative.

Importance of the Water and Wastewater Infrastructure on Health and the Economy

The WWS is vital for the humans' health and well-being. Cali and others discussed the importance of protecting the WWS from cyber threats as WWS is a fundamental service essential for sustaining life and maintaining public health. The WWS ensures the delivery of clean and safe water to its end-users for cooking, drinking, and hygiene, which are all vital for preventing disease and promoting health. The removal of wastewater removes the impurities or contaminants and distributes them to the appropriate sources for further processing. Cyberattacks interrupting this process can disrupt the processes within the system, which can be fatal.

Research provided by Watkins et al. and Alladi informed of recent attacks on the WWS and the possible disastrous consequences. Watkins and others described the cyberattack on Florida's Oldsmar Water Treatment Facility. The threat actor was able to leverage compromised credentials and access the software TeamViewer and attempted to increase the levels of sodium hydroxide in the water supply. Increasing sodium hydroxide within the water supply can cause skin burns and internal damage if ingested. Alladi's description of the attack on the Kemuri Water Treatment Facility was similar to that of the APT group, which successfully controlled and altered the quantity of chemicals used in water treatment. Luckily, there were no reported health concerns from the breach, but the time to replenish water supplies was impacted and negatively affected businesses.

Pamidimukkala and others also outlined the importance of WWS as it is multifaceted and ensures safe and clean water for the healthy functioning of society. In addition, the WWS regulates environmental pollution as it manages wastewater collection, treatment, and disposal. The WWS endorses social well-being, as access to water enhances the quality of life and supports various activities such as recreation. The authors also noted how the WWS is essential

to disaster response and recovery, as a resilient WWS will ensure uninterrupted access to water during natural disasters. Pamidimukkala and colleagues also indicated that the WWS needs to adapt and expand to meet the community's growing needs and ensure that future generations can access clean water and sanitation services to maintain health and economic stability.

The WWS is vital to any region's economic growth and stability. Of course, an attack on any WWS would have catastrophic consequences, making the WWS a vulnerable target to both threat actors and nation-state APTs. Pamidimukkala et al. described the ripple effect within a region's economic structure when the WWS is compromised. Businesses rely on water and water treatment for their agriculture, manufacturing, and tourism operations. In addition, when water sources cause illness from waterborne diseases, healthcare costs increase, negatively affecting the critical infrastructure of healthcare and public health. Pamidimukkala and others also noted that areas negatively impacted by cyberattacks appeared to have unreliable water and wastewater services, which would deter investments, decrease property values, and slow economic growth.

Lis and Mendel agreed with Pamidimukkala et al.; however, they described additional indirect economic effects of an attack on the WWS. For instance, Lis and Mendel reported disruptions to supply chains and economic activity, tax revenue losses, and increased business costs secondary to enhanced government policies. They also revealed higher water prices to end users as enhanced security and insurance costs incurred by water utilities. Himmat also indicated that cyberattacks on any organization will cost money as national governments continue to develop and invest in cybersecurity strategies. However, cyberattacks have led national governments to reexamine their perceptions of cybersecurity risks and the potential impacts on society, the economy, and critical infrastructure. Owen wrote how cyberattacks have cost millions of dollars in damages, which can significantly impact the financial stability of water

utilities. Owen also added that past cyberattacks have cost millions of dollars in damages, which can significantly impact the financial stability of water utilities. Lis and Mendel stated that the integrity and resilience of the WWS are vital for public health and environmental protection and sustaining economic stability. Therefore, it is essential to protect systems that assist critical infrastructures, such as industrial control systems (ICS), and IT systems protecting systems that assist critical infrastructures, such as ICS and IT systems, is essential. The Critical Role of Information Technology Systems & Protecting Critical Infrastructures

Miller and Rubio et al. emphasized the importance of protecting ICS as they described how essential it is to control and manage industrial processes. The authors explained that ICS has continually evolved with technology's complexity and connectivity, and its interconnectivity presents new vulnerabilities and cybersecurity challenges, such as IoT and cloud computing. Moreover, technological advancements have allowed threat actors and APTs more opportunities to cause operational shutdowns, financial loss, equipment damage, and the potential loss of human life. Furthermore, Miller noted a change in attack motives from personal attack motives to more political ones following 2009. Nation-state-backed resources for threat actors and APTs became more abundant as ICS became more interconnected and technology progressed. Skiba also warned how the water utility infrastructure has advanced in terms of the technical control systems that manage and track infrastructure properties. He concurred with Miller and Rubio et al. that these systems are currently more vulnerable due to their complexity and internet connectivity.

Protecting IT systems is vital to protecting the 16 critical infrastructures, especially the WWS. Dawson and others reverted to protecting the IT systems as they are vital for protecting the 16 critical infrastructures. The role of the IT system is dynamic as it is responsible for the

WWS control, communication, and operations, which enable operational control through its SCADA. IT is imperative as it ensures security and resilience against cyber threats while complying with cyber security standards and regulations. Research has revealed several breaches secondary to outdated SCADA systems, such as the Kemuri Water Facility and the San Francisco Bay Area Water Facility cyberattacks. Therefore, updated and maintained IT and ICS systems are also essential for defending the WWS and mitigating cyberattacks.

How do APT groups target the United States' critical infrastructures, and why is understanding and implementing effective defense strategies essential for deflecting these threats?

APTs and Cyberattacks

Lehto and Neittaanmaki described how APTs are growing and pose a significant threat to critical infrastructure and cyber-physical systems. Cyberattacks conducted by nation-state-sponsored APTs focus on maintaining ongoing access to a targeted network and obtaining data. Targeted data includes, but is not limited to, intellectual property, business contracts, negotiations, secret policy, military papers, and other sensitive information. In addition, information regarding political, military, or financials is considered high-value. Attacks executed by APT groups are stealthy and sophisticated and target valuable secret information. These attacks can manipulate data, which are thought to be the most dangerous, as these can corrupt or override valuable data and make detecting the responsible APT difficult.

As Lehto and Neittaanmaki noted, APTs that are more difficult to detect successfully achieve their objectives. Sharma also expanded on APTs' stealthy nature and wrote about organizations' various challenges when identifying responsible APTs. Sharma believed using more sophisticated and advanced TTPs allows APTs to remain incognito during and after attacks. For example, stealthier and more evasive malware is becoming more common and more

problematic for cybersecurity professionals to detect. Furthermore, the malware is more precise, assisting APTs with evading detection, especially by organizations that use outdated ICS and IT systems. As mentioned in the former, the Kemuri Water Facility and the San Francisco Bay Area Water Facilities fell victim to cyberattacks secondary to outdated instrumentation. Sharma noted that organizations need equipment that can analyze large volumes of network traffic, identify cyber threats, and defend against potential attacks. Nation-state-endorsed APTs utilize social networking and other OSINT capabilities to identify victims' interests. Identifying APTs when their goals and objectives are unclear is more challenging.

Lehto and Neittaanmaki also discussed the several distinct phases of a cyberattack and the various models of APT attacks published by MITRE ATT&CK, Mandiant Attack Lifecycle Model, LM Cyber Kill Chain, Unified Kill Chain, and Hybrid Cyber Kill Chain. Of course, Lehto and Neittaanmaki believed that utilizing a model makes identifying or detecting a cyberattack easier. Regardless of the various models and frameworks, threat actors continually find innovative ways to evade detection. Brooks wrote about addressing the vulnerabilities and challenges of securing CIs, particularly water and wastewater treatment facilities, from cyber threats and threat actors. Brooks believed that even with beneficial resources such as NIST, RMF, and NIPP-RMF, challenges remain in detecting TTPs and securing the WWS.

Targeting Critical Infrastructures

Sharma, Brooks, and Riggs et al. continually illustrated the innovations and sophistication of cyberattacks by nation-state-endorsed APTs. Sharma noted that these APTs target critical infrastructures like the WWS due to their strategic importance and potential impact on national security. Sharma, Baharami, and The Joint Cybersecurity Advisory reported spear phishing as one of the most used TTPs, as threat actors can send emails with attachments or

infected links with malware. However, authors such as Lanz and Malatji described that TTPs like ransomware, denial of service attacks, watering hole attacks, and cryptography are alternatives when attacking critical infrastructures, namely the WWS.

Alkhaldi and others discussed the SolarWinds attack and how threat actors and APT groups have advanced with cyber attacks. Although the SolarWinds attack did not target critical infrastructures directly, several other supporting agencies fell victim to the attack. Agencies such as the Department of Commerce, DoD, DOE, National Institutes of Health, Department of the Treasury, and the Department of State support the U.S. critical infrastructures. Alkhaldi et al. explained how the malware was distributed to SolarWinds clients and utilized to create backdoors for threat actors to access a more extensive system of SolarWinds' clients. The SolarWinds breach affected approximately 18,000 clients, including many supporting federal agencies to critical infrastructures such as the WWS, validating the effectiveness of the attack.

Understanding Threat Actors, Attacks, and Defensive Measures

As Owen's research stated, understanding cyberattacks and cyber threats is imperative to establishing effective defense strategies when protecting the WWS. Moreover, Owen explained how cyber threats evolve, making critical infrastructures more vulnerable to cyberattacks. For example, SCADA systems are essential; they can control and monitor the infrastructural processes that WWS utilizes to operate. Therefore, increased investment in cybersecurity is imperative, as cyberattacks targeting the WWS can cause physical harm, information breaches, economic decline, and even loss of life. Having a better understanding of how critical infrastructures operate will allow for better cyber defenses.

Dawson's beliefs also aligned with Owen's, as he also mentioned the importance of understanding IT systems. These systems are essential for these infrastructures' control,

communication, and operations, enabling operational control through SCADA Systems. Employee education regarding SCADA and IT systems will assist organizations in protecting themselves from cyberattacks. Moreover, as mentioned during the Kemuri Water Utilities cyberattack by Alladi et al., the Syrian hacktivist group could have caused more damage to those within the region if they had obtained a deeper understanding of SCADA systems and how they work. Therefore, a thorough understanding of SCADA and IT systems is essential for cyberattacks and, more importantly, cyber defenses.

Additional research by Adeptu and others also revealed the need to understand and proactively establish cybersecurity defense strategies for safeguarding the WWS and other critical infrastructures. However, these authors believed that to defend critical infrastructures effectively, proactively, and efficiently from cyberattacks, they must thoroughly understand the organization's response time. Knowledge of time and response to cyberattacks will yield more robust defense strategies, which will mitigate cyberattacks effectively. For example, the Syrian hacktivist group increased the time it took to provide water supplies to end users because the SCADA system was outdated, and the response time to the attack was slow during the Kemuri Water Utilities cyberattack. In comparison, Watkins et al. highlighted the importance of timely responses during the cyberattack on the Oldsmar Water Treatment Facility in Florida. If the cyberattack had not been detected and mitigated in a timely fashion, the threat actor could have increased sodium hydroxide levels in the water supply from 100 ppm to 11,000 ppm, which is over 100 times the required amount, causing physical harm. Lastly, Buchannan explained how an operator quickly identified and mitigated a cyberattack on the San Francisco Area Water Facility, stopping the threat actor from accessing the human-machine interface. Buchannan recognized the need to secure operational and information technology systems promptly.

McCarthy and Miller brought attention to technological advances in their research and the effects of cyberattacks. Both authors mentioned how ICS and IT systems are increasingly becoming more innovative secondary to the increasing adoption of network-enabled technologies in critical infrastructures such as the WWS. However, with increased technological advances, such as automation, sensors, data collection, and network devices becoming more integrated, vulnerabilities continue to increase. Furthermore, Miller reviewed how APT groups and threat actors utilize credential harvesting, phishing campaigns, and man-in-the-middle attacks to gain unauthorized access to networks and compromise data integrity. Grubbs and colleagues discussed how threat actors could deploy ransomware, which negatively affected the city's ability to function on several levels, including water utility. Because of technological advances, the threat actors could damage or encrypt approximately 40% of its servers and 20% of its laptop and desk computers. Hasanzadeh described how the Rye Brook Water Utility also experienced a ransomware attack. Although the facility had layers of protection, the utilities IT system was still penetrable, as evidenced by the attack, suggesting the need for continued advancements and improvements with cyber defense strategies and mitigation for the WWS.

Limitations of the Research

Several limitations of this research exist, such as the methodologies used by APT groups and the lack of academic resources targeting mitigation strategies concerning specific TTPs. Several articles mentioned the evolution and anatomy of APT cyberattacks, but few mentioned or expanded on the TTPs utilized, like phishing emails and ransomware. Furthermore, a more detailed analysis of the execution of payloads and the associated APT groups would provide a comprehensive overview of each attack. Moreover, each attack is generalized, except for some attacks pertaining to specific infrastructures like the WWS. Generalizations may not be pertinent

to all 16 critical infrastructures. The research also lacked specific mitigation strategies related to each attack. Successful and unsuccessful mitigation strategies will encourage and cultivate future research targeting specific TTPs, ATP groups, and the TTPs utilized, as well as effective mitigation strategies.

Future Research Recommendation

After conducting this research, there are many unanswered questions and topics that require further exploration. Future research might focus on how the U.S. could effectively defend itself from attacks targeting critical infrastructures like the WWS, investigate specific vulnerabilities and consequences, and compare the key relationships between nation-state cyberattacks and geopolitical and economic factors.

How can the United States effectively defend against emerging technologies and risks?

The research provided examples of cyber threats and cyberattacks; however, many authors mentioned little information regarding defending against such attacks. While some sources mentioned mitigation techniques, there is much room for improvement. Research regarding the collaboration between the private and public sectors necessitates a more profound understanding of how APTs successfully execute cyberattacks to identify vulnerabilities and the most effective defensive strategies. For example, organizations should compare and contrast cyberattacks to identify system vulnerabilities and organizational failures, such as lack of employee education. Research should incorporate conventional TTPs in conjunction with technological advances like AI.

What Specific Effective Mitigation Strategies Can Protect the WWS from TTPs?

Much of the research targeted specific attacks by APTs and vulnerabilities of the WWS. However, many sources should have mentioned effective mitigation strategies to protect from

these cyberattacks. In addition, these sources should have mentioned what mitigation strategies were in place and failed during some cyberattacks. Many articles reported the cyberattack, the cause of the attack, and vulnerabilities. Data regarding effective mitigation strategies could assist with cyber defense strategies and identifying which APT groups are responsible for a specific cyberattack. Furthermore, analyzing data regarding effective and ineffective mitigation strategies will allow for the development of defense mechanisms that will counteract unique cyber threats.

How Do Human Factors and Behavioral Analysis Affect Cyberattacks?

There is a need for further research to examine how human factors and behavioral analysis can be applied to understand insider threats, social engineering tactics, and human vulnerabilities within critical infrastructure organizations, such as the WWS. Often, cyberattacks are secondary to a current or disgruntled former employee, as evidenced in Kansas's Post Rock Water District attack. Also, research regarding human vulnerabilities within critical infrastructure organizations is strongly recommended. The understanding of why employees impulsively click on malicious links is demonstrated in the Rivera Beach Water Utility cyberattack. Having a better understanding as to why people impulsively click on links and insider threat actors will assist in defending critical infrastructures and organizations from cyberattacks.

Conclusion

This research examined TTPs utilized by threat actors and APT groups during cyberattacks targeting critical infrastructures such as the WWS. There was evidence as to how each attack negatively caused or could inflict physical harm, promote economic instability, cause health concerns, or even death to end users within each provided example. The insights and experiences shared by various authors provided insight into the escalating cyber threats and

attacks faced by the U.S. and the possible consequences of successful cyberattacks on critical infrastructures such as the WWS.

The targeted attacks on WWS and systemic vulnerabilities discussed in the provided examples underscore the urgent need for vigorous cybersecurity measures and proactive defense strategies to thwart evolving threats. With their specific objectives and advanced tactics, APTs target critical infrastructures with the intent of compromising data, disrupting operations, and causing damage. However, understanding the various phases of APT cyberattacks, the rigorous challenges of detecting APT activities, and the TTPs employed by threat actors highlight the critical role of effective defense strategies. Implementing aggressive cybersecurity measures, enriching staff education, and increasing funding for advanced technologies are critical to protect critical infrastructures from APTs, cyber threats, and cyberattacks.

A core problem and common theme throughout the research was the accessibility to utilities' systems, as evidenced by several examples of cyberattacks on the WWS. Many articles reported that water utilities used outdated IT and SCADA systems, allowing threat actors easy access to system networks. Updating and hardening these systems would have prevented access to these systems. In addition, threat actors used stolen employee credentials to access the system's controls, as reported in the examples of cyberattacks. Phishing and social engineering were other standard methods, as threat actors used emails laced with malware or ransomware to deliver their payload and infect a system network. Regardless of the TTPs used, the research provides clear evidence of increased attacks targeting the WWS.

Protecting U.S. critical infrastructures, like the WWS, is imperative. These infrastructures are essential for public health, economic stability, and the overall well-being of end users. Keeping critical infrastructure resilient and secure is essential to maintaining operational

continuity, preventing disruptions, and minimizing cyber-related risks. Considering the increasing cyber threats and the potential consequences of successful attacks on critical infrastructures, continuous efforts are essential to improve cybersecurity defenses, enhance threat intelligence, and foster stakeholder collaboration. Cybersecurity must be understood and prioritized, with the implementation of aggressive, proactive measures to safeguard all critical infrastructures within the U.S.

References

2023 threat roundup. Forescout. (2024).

2023 year in Review: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.).

Advanced persistent threats and nation-state actors. Advanced Persistent Threats and Nation-State Actors | Cybersecurity and Infrastructure Security Agency CISA. (n.d.).

Adepu, Sridhar & Palleti, Venkata & Mishra, Gyanendra & Mathur, Aditya. (2019). Investigation of Cyber Attacks on a Water Distribution System.

Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021). Solar winds hack: In-depth analysis and countermeasures. *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*.

Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial Control Systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*, 1–8.

Aslam, M. M., Tufail, A., Kim, K.-H., Apong, R. A., & Raza, M. T. (2023). A comprehensive study on cyber attacks in communication networks in water purification and distribution plants: Challenges, vulnerabilities, and future prospects. *Sensors*, *23*(18), 7999.

Bahrami, P. N., Ali Dehghantanha, A., Tooska Dargahi, T., Parizi, R., Choo, K.-K. R., & Javadi, H. (2019). Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. *J Inf Process Syst*, *15*(4), 865–889.

Bhaiyat, H., & Sithungu, S. (2022). Cyberwarfare and its effects on critical infrastructure. *International Conference on Cyber Warfare and Security*, *17*(1), 536–543.

Brooks , C. (2019). Critical Infrastructure Protection at the Local Level. *Cyber Conflict During Competition* , 45–64.

Buchanan, S. S. (2022). (rep.). *CYBER-ATTACKS TO INDUSTRIAL CONTROL SYSTEMS SINCE STUXNET: A SYSTEMATIC REVIEW* (pp. 1–138). East Eisenhower Parkway, MI: ProQuest.

Cali, Ü., Catak, F. Ö., Balogh, Z. G., Ugarelli, R., & Jaatun, M. G. (2023). Cyber-physical hardening of the digital water infrastructure. *European Interdisciplinary Cybersecurity Conference*.

Center for strategic and international studies. CSIS. (n.d.).

Cervini, J., Rubin, A., & Watkins, L. (2022). Don't drink the Cyber: Extrapolating the possibilities of Oldsmar's water treatment cyberattack. *International Conference on Cyber Warfare and Security*, *17*(1), 19–25.

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021a). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*, *26*(1), 69–75. https://doi.org/10.2478/raft-2021-0011

González-Manzano, L., de Fuentes, J. M., Ramos, C., Sánchez, Á., & Quispe, F. (2022). Identifying key relationships between nation-state cyberattacks and geopolitical and economic factors: A model. *Security and Communication Networks*, *2022*, 1–11.

Grubbs, R., Stoddard, J., Freeman, S., & Fisher, R. (2021). Evolution and trends of Industrial Control System Cyber Incidents since 2017. *Journal of Critical Infrastructure Policy*, *2*(2), 45–79.

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5).

Himmat, M., Ibrahim, M. A., Hammam, N., Eldirdiery, H. F., & Algazoli, G. (2023a). The current trends, techniques, and challenges of cybersecurity. *European Journal of Information Technologies and Computer Science, 3*(4), 1–5.

Himmat, M., Ibrahim, M. A., Hammam, N., Eldirdiery, H. F., & Algazoli, G. (2023b). The current trends, techniques, and challenges of cybersecurity. *European Journal of Information Technologies and Computer Science, 3*(4), 1–5.

Horne, J. (2023, December 21). *A cyber threat to U.S. drinking water*. Default. https://www.lawfaremedia.org/article/a-cyber-threat-to-u.s.-drinking-water

Incident response guide: Water and wastewater sector - CISA. (n.d.-a).

Lanz, Z. (2022). Cybersecurity risk in U.S. Critical Infrastructure: An Analysis of publicly available U.S. government alerts and Advisories. *CrimRxiv*.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. *Computational Methods in Applied Sciences*, 3–42.

Li , C. (2022). Securing US Critical Infrastructure against Cyber Attacks. *In Harvard Model Congress Boston 2022*, 1–20.

Lis, P., & Mendel, J. (2019). Cyberattacks on Critical Infrastructure: An Economic Perspective. *Economics and Business Review, 5*(2), 24–47.

Lloyd Owen, D. (2021). Cybercrime, cybersecurity and Water Utilities. *International Journal of Water Resources Development, 37*(6), 1021–1026.

Malatji, M., Marnewick, A. L., & Von Solms, S. (2021). Cybersecurity capabilities for Critical Infrastructure Resilience. *Information & Computer Security, 30*(2), 255–279.

Managing u.s.-china tensions over public cyber attribution. (n.d.-b).

McCarthy , J., Stea , B., & Faatz, D., CYBERSECURITY FOR THE WATER AND WASTEWATER SECTOR (2023). McLean, VA ; Mitre.

Moraitis, G., Nikolopoulos, D., Bouziotas, D., Lykou, A., Karavokiros, G., & Makropoulos, C. (2020). Quantifying failure for critical water infrastructures under cyber-physical threats. *Journal of Environmental Engineering*, *146*(9).

Ongoing cyber threats to U.S. water and wastewater systems - CISA. (n.d.-c). https://www.cisa.gov/sites/default/files/publications/AA21-287A-Ongoing_Cyber_Threats_to_U.S._Water_and_Wastewater_Systems.pdf

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for Cyber-Secure Critical Infrastructure. *Sensors*, *23*(8), 4060.

Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, *35*, 100464.

Pamidimukkala, A., Kermanshachi, S., Adepu, N., & Safapour, E. (2021). Resilience in water infrastructures: A review of challenges and adoption strategies. *Sustainability*, *13*(23), 12986.

Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in Industrial Control Systems. *Computers & Security*, *87*, 101561.

Sasipriya, S., Madhan Kumar, L. R., Raghuram Krishnan, R., & Naveen Kumar, K. (2021). Intrusion detection system in web applications (IDSWA). *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*.

Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2023). Advanced persistent threats (APT): Evolution, anatomy, attribution and countermeasures. *Journal of Ambient Intelligence and Humanized Computing*, *14*(7), 9355–9381.

Shawe, R., & McAndrew, I. R. (2023). Increasing threats to United States of America infrastructure based on Cyber-Attacks. *Journal of Software Engineering and Applications*, *16*(10), 530–547.

Shlapentokh-Rothman, M., Kelly, J., Baral, A., Hemberg, E., & O'Reilly, U.-M. (2021). Coevolutionary modeling of cyber attack patterns and mitigations using public datasets. *Proceedings of the Genetic and Evolutionary Computation Conference*.

Skiba, R. (2020a). Water industry cyber security human resources and training needs. *International Journal of Engineering Management*, *4*(1), 11.

Skiba, R. (2020b). Water industry cyber security human resources and training needs. *International Journal of Engineering Management*, *4*(1), 11.

Traffic light protocol (TLP) definitions and usage: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024a, February 14).

Water and wastewater sector - incident response guide: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024b, February 2).

Water and wastewater systems. Water and Wastewater Systems | Cybersecurity and Infrastructure Security Agency CISA. (n.d.).

West, T., & Zentner, A. (2019). Managing security risks: An assessment of U.S. critical cyber infrastructure protection. *SSRN Electronic Journal*.