AUTHOR: YANIR LAUBSHTEIN

PROTECTING WATER AND SANITATION INFRASTRUCTURE FROM CYBERTHREATS

A CYBERSECURITY STUDY FOR LATIN AMERICA AND THE CARIBBEAN

EDITORS:
ARIEL NOWERSZTERN • MARCELLO BASANI • FERNANDO MELEAN • HILA COHEN MIZRAV

IDB
IDB | LAB

Protecting Water and Sanitation Infrastructure from Cyberthreats

A Cybersecurity Study for Latin America and the Caribbean

Author:
Yanir Laubshtein

Editors:
Ariel Nowersztern
Marcello Basani
Fernando Melean
Hila Cohen Mizrav

IDB

WITH THE COLLABORATION OF

SOURCE OF INNOVATION

This publication is part of Source of Innovation, a partnership promoted and co-financed by the Water and Sanitation Division of the Inter-American Development Bank (IDB) and IDB Lab in coordination with key partners such as the Government of Switzerland, through the State Secretariat for Economic Affairs (SECO), the FEMSA Foundation, the Government of Korea, through its Ministry of Environment, and the Government of Israel.

JEL codes:
H12, K24, L95, M15, N56, O32, O33, Q25.

Keywords:
Water, sanitation, wastewater, water treatment, critical infrastructure, operational technology, industrial control systems, Industry 4.0, cybersecurity, cyber policies, cyberspace, cyberattacks, cyberthreats, incident response, strategic planning, data protection.

The opinions expressed in this work are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.

Table of Contents

3 Water and Sanitation Sector Preparedness in Latin America and the Caribbean

List of Tables and Figures

Acknowledgments

This publication is part of the knowledge agenda developed by Source of Innovation, a partnership promoted and co-financed by the Water and Sanitation (INE/WSA) Division of the Inter-American Development Bank (IDB) and IDB Lab in coordination with key partners, such as the Government of Switzerland, through the State Secretariat for Economic Affairs (SECO), the FEMSA Foundation, the Government of Korea, through its Ministry of Environment, and the Government of Israel. In collaboration with this partnership, the study was also co-developed with help of the cybersecurity team of the Innovation in Citizen Services (IFD/ICS) Division of the IDB.

The generated knowledge product seeks to show readers the cybersecurity trends, challenges and opportunities in the water and sanitation sector of Latin America and the Caribbean (LAC), assessing LAC's water and wastewater infrastructure cybersecurity readiness and presenting key recommendations for public and private sector actors to increase their organization's overall cyber resilience.

The authors would like to thank all the people who participated in the review and enrichment of this document, in particular peer reviewers María Donoso, James Pichardo and Iván Rodríguez. Special acknowledgement is also made to Ricardo Poppi, Kim Olson and Clara Sarcone for their contributions and commendable work in proofreading and editing the text. Last but not least, the IDB also wishes to thank the organizations and professionals who kindly agreed to take part in our interviews and consultations, providing valuable insight necessary for the completion of this publication.

Acronyms

APT: Advanced persistent threat

CBMs: Confidence building measures

CERT.br: Brazilian National Computer Emergency Response Team

CI: Critical infrastructure

CIA Triad: Confidentiality, integrity, and availability model

CMM: Cybersecurity Capacity Maturity Model for Nations

CPS: Cyber-physical systems

CSO: Combined sewer overflows

EU: European Union

EUISS: EU Institute for Security Studies

ICS: Industrial control systems

ICT: Information and communication technology

IDB: Inter-American Development Bank

IIoT: Industrial Internet of things

IoT: Internet of things

IT: Information technology

LAC: Latin America and the Caribbean

NCSC: UK National Cyber Security Centre

NCSS: National Cybersecurity Strategy

NIST: US National Institute of Systems and Technology

OAS: Organization of American States

OT: Operational technology

PLC: Programmable logic controller

PPP: Public-private partnerships

SCADA: Supervisory control and data acquisition

SSO: Sanitary sewer overflows

W&S: Water and sanitation

Preface

Digitization is a key element for 21st century governance, helping States to improve the quality and coverage of the public services they provide, as well as to increase the integrity of their activities for the benefit of society.

While the COVID-19 pandemic has served as a recent accelerator for digitization, both the public and private sectors began the 21st century with significant investment efforts in technological infrastructure, digital systems and human talent, seeking to improve their management and services. Citizens have been able to easily and efficiently access more services and information, using innovative channels of communication with governments and businesses.

Aware that digitization is a tool that promotes efficiency, agility, and transparency in the operation of the public sector, and that it also contributes to improving the quality of life of the population of Latin America and the Caribbean, from the Inter-American Development Bank we promote the implementation of digital technologies in the countries of the region.

Along with the opportunities described, this digitization process brings with it complexities and challenges. As the digitization of urban infrastructures and services increases, so does their exposure to the inherent risks and vulnerabilities of cyberspace, opening the door to malicious actors and cyberattacks that seek to damage critical areas such as water and sanitation (W&S) (Guillaume, 2022), health, energy, transportation, among many others.

In this context of critical infrastructure, digitized W&S systems are classified as one of the most sensitive (IWA, 2022), due to their intrinsic relationship with the health of the population and hygiene controls, encompassing responsibilities such as the production and continuous supply of drinking water for citizens, along with the collection, transportation and treatment of wastewater, among other processes that are fundamental for the sanitary conditions of residential and public areas. Given the criticality of these operations, it is not surprising that a report by the American Water Works Association has named cyber risk as the number one threat facing the W&S sector (Germano, 2019).

A cyberattack directed at W&S sector dependencies has the capacity to hinder or even interrupt the operations of entire cities, causing significant and, in certain cases, irreparable or catastrophic damage to State technology systems, leaving the population without water supply for periods of several hours or even days, and increasing the risk of contracting diseases associated with the ingestion of untreated or contaminated water. Thus, endangering people's lives.

At the same time, certain traditional practices of digitized infrastructures, such as monitoring, data collection and extensive record keeping, can be exploited by cybercriminals seeking to gain possession of confidential information from such water treatment facilities for illicit purposes, such as disclosing customer and supplier data, finding vulnerabilities in the managing body of the company or the State, disrupting the supply chain, or even selling the information to competitors on the black market.

The reasons why W&S infrastructure faces these types of threats on a daily basis are as varied as the attack methods used by cybercriminals. Personal, political and economic interests, among others, drive criminals to develop new tools and methods, studying these systems and finding vulnerabilities that in time will allow them to increase the frequency and sophistication of said incidents.

To counter these threats, it is the responsibility of administrations to proactively plan and invest to ensure that cyberattacks do not cause disruptions in their management and endanger the population. Investment in cybersecurity is the primary mechanism to fulfill this objective of defending and supporting the digitization of these critical entities for the health of their users and the digital services they possess.

This study aims to provide an overview of the cyber protection that the countries of the region implement within their entities for the collection, treatment and distribution of water that operate within their national territory. It provides information compiled from various sources, experts and publications, based on which a comprehensive analysis of the preparedness level of the sector is presented, with emphasis on the importance of protecting these critical infrastructures within the environment of the Fourth Industrial Revolution (Stankovic, Hasanbeigi and Neftenov, 2020).

Introducing arguments such as the cost of cybercrime, trends in the region, the main incentives and challenges at the international level, among others, it draws on the experience of countries with recognized cybersecurity policies such as Israel and the United Kingdom to present case studies detailing the results of solid management committed to information security in the sector. Based on the analysis of all these experiences and recommendations, the study is proposed as a tool to promote knowledge and key cyber defense actions to ensure the future of the W&S sector.

At the IDB, we are well aware of these challenges, and for this reason we are working closely with W&S providers and governments in the region, supporting secure digitization that strengthens their cybersecurity capabilities. The implementation of comprehensive cybersecurity policies will make it possible to enjoy the benefits of the Fourth Industrial Revolution, guaranteeing the well-being of the population. We invite you to join us in this effort.

Roberto de Michele
Innovation in Citizen Services Division Chief
Institutions for Development Sector
Inter-American Development Bank

Sergio Campos
Water and Sanitation Division Chief
Infrastructure and Energy Sector
Inter-American Development Bank

Executive Summary

The water and sanitation sector is essential for livelihoods and has therefore been recognized by most countries as critical infrastructure (WHO, 2019). While the growing trend of automation and digitalization of W&S sector facilities improves efficiencies and helps reduce operating costs, it also exposes the sector's facilities and operations to ever-increasing cyber risks. The number and variety of cyberthreats and malicious actors who target utilities is rapidly increasing: from nation-state actors seeking to cause political and social chaos as well as disrupt economies, cybercriminals looking for profit, hacktivists driven by ideological or personal agendas, and disgruntled insiders to individuals attempting to get a break on their bills.

As digital technologies spread and add greater value to W&S infrastructure, cybercriminals try to exploit the interconnected infrastructure by attacking industrial control systems (ICS), the specialized computers that manage flow operations, wastewater treatment, and more. Cyberattacks will escalate in frequency, volume, and sophistication. However, limited awareness coupled with a reluctance to invest in cybersecurity due to its costs, along with a lack of attention and regulatory requirements, will result in utilities' underinvestment in cybersecurity and elevated vulnerability to cyberattacks – a result that may have harsh consequences.

Water utilities around the world have already faced a wide range of attacks, from ransomware and tampering with ICS to manipulating valve and flow operations, affecting chemical treatment formulations, along with other attempts to potentially damage machinery and disrupt operations. Interviews conducted over the course of this study revealed that some entities in Latin American and the Caribbean have already suffered a cyber event that affected their operations, although recovery was quickly achieved. Nonetheless, an entity's very ability to classify an operational event as a cyber incident greatly depends on its digital infrastructure, forensic capabilities, and cyber awareness.

Cyberattacks that target W&S sector systems could compromise drinking water supply, water quality, or wastewater collection and treatment by disrupting business or process continuity and reliability. Such attacks could also manipulate consumption information, interfere with billing, and compromise customer data. Cyberattacks on entities that manage water or wastewater can have devastating effects on public health, the environment, and the economy. In addition, cyberattacks resulting in contamination, operational malfunction, or service outages can ultimately erode customer trust and even result in financial and legal liability.

This document is the first of its kind published by the Inter-American Development Bank to examine cyberthreats in the LAC W&S sector, which are cause for increasing concern. The IDB, together with the Organization of American States (OAS) conducted wide-ranging studies to assess the cyber maturity of each LAC country in 2020, using the Cybersecurity Capacity Maturity Model for Nations, known as the CMM model. The IDB publishes general-interest cybersecurity guides as well as cybersecurity best practices guides for other critical sectors such as electricity, healthcare, and smart cities. This document also adds to the latest knowledge available in the LAC W&S sector, made publicly by the IDB, touching on wide-ranging issues including the sector's digital transformation.

This report reviews W&S sector technologies and explains the cyberthreats facing water infrastructure technology. It assesses LAC's W&S sector cybersecurity readiness using written material and interviews with key representatives of public sector institutions and other water utilities in LAC. Finally, it presents a series of recommendations for public and private sector actors. Additionally, a free online self-assessment questionnaire was implemented to allow organizations to assess their current cybersecurity posture, identifying existing gaps and providing recommendations.

Effective cybersecurity in the W&S sector requires not only implementing technical measures and following methodologies but prioritizing and integrating cybersecurity in corporate management and culture. This would strengthen the sector's cybersecurity, allowing for the safe, uninterrupted provision of essential water and sanitation services to people in LAC.

KT Stock photos / shutterstock.com

1 Introduction

Conceptual Framework

What Are Cyberthreats?

The rapid ongoing development of technology along with our increasing dependence on it, has in recent years led to a new threat, which affects all areas of life: the cyberthreat. Today, many means are controlled and supported by information technology systems, exemplified by water and electricity systems, telecommunications, and transportation. This fact poses new technological challenges to governments, companies, organizations, and citizens of countries all over the world.

This domain is known as cyberspace. According to the Computer Security Research Center (CSRC) of the US National Institute of Systems and Technology (NIST), cyberspace can be described as the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries (CSRC, 2022a).

What Is a Cyberattack?

The CSRC (2022b) defines cyberattack as an attack, via cyberspace, that targets an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure, destroying the integrity of the data, or stealing controlled information.

Some cyberattacks are carried out by exploiting vulnerabilities in any technological platform. A vulnerability is a technological weakness or unintended behavior in a computer system that allows potential attackers to gain access to it or perform actions they should not be allowed to perform. Vulnerabilities allow for various levels of unauthorized access to an information system, which attackers can then use to carry out a range of actions depending on their objectives and intentions. There is a distinction between vulnerabilities that have been exposed and for which software developers have released a security update that prevents them from being exploited, the "known vulnerabilities," and vulnerabilities that have been exposed by researchers but lack any security update to prevent them from being exploited, the "Zero-Day" vulnerabilities. In the face of the latter, software developers have virtually zero days to develop a security update before the vulnerability could be exploited for malicious purposes (Ablon and Bogart, 2017).

Bayazed / Shutterstock.com

Defining Critical Infrastructure

On the national scale, infrastructure is characterized as critical when it is believed its failure will cause a substantial socioeconomic crisis, potentially destabilizing society and carrying political, strategic, or security ramifications. Different countries define critical infrastructure (CI) differently, but what they all have in common, in our context, is that it is an infrastructure with a computerized dimension on which other physical systems rely, and whose failure to function can cause substantial damage to the physical dimension (Tabansky, 2011). For water infrastructure, that damage may extend beyond the socio-political system to affect actual physical structures (dams, distribution systems, etc.) and the environment.

In some countries, the definition of CI is based on the infrastructure's formal designation, while in others, it is based on the societal consequences of the damage to it. For example, the European Union (EU) defines CI as systems that are necessary for the national and cross-border security of essential services belonging to sectors such as information and communication technology (ICT), energy, finance, health, and transport (ENISA, 2023). In the United States, the term critical infrastructure refers to systems, assets or networks (physical or virtual) that are crucially important, therefore their destruction would have serious consequences for national security in general, and economic security in particular, as well as for public health (CISA, 2023). Since countries define CI differently, sectors where this infrastructure can be found vary as well. According to the US Cybersecurity and Infrastructure Security Agency (CISA), CI systems can be found, among others, in the energy sector, the food and agriculture sector, the communications sector, transportation systems, and the water and wastewater systems sector (CISA, 2022).

Many CI systems are managed and operated through digital control and monitoring systems known as supervisory control and data acquisition (SCADA), which mediate between the physical world and cyberspace through programmable logic controllers (PLC). SCADA systems allow remote access in some cases. As for water systems, it is often possible to remotely control the operation and shutdown of pumps that draw water from water reservoirs depending on needs and the amount of water in the reservoir, in addition to controlling water flow in the dams and if necessary, their closure (Stouffer et al., 2015).

American Public Power Association/ Shutterstock.com

The Rise of OT Systems

The hardware and software used with automation control systems within the infrastructure is referred to as operational technology (OT) (Murray, Johnstone and Valli, 2017). OT systems are used worldwide to control and monitor industrial processes in critical utilities and infrastructure, such as power stations, nuclear plants, and water and sewage infrastructure.

Over the past decade, the rise of the industrial Internet of things (IIoT) resulted in the convergence of Information Technology (IT) and OT. Industries connected IT and OT systems in an effort to improve infrastructure functionality thus eliminating so-called air gaps that had protected their OT systems from hackers and malware originating from the wider Internet. Facilitated by air gap elimination, hostile actors have increased their hacking efforts against OT systems to obtain data, disrupt operations, or launch cyber terror attacks against CI (Siboni, Cohen and Rotbart, 2013). These risks are growing with the ever-increasing number of connected devices, many of which are not secured by their manufacturers or users, as well as an increase in the occurrence of service disruption attacks on public and private systems, along with extortion and ransom demands (Siboni, Cohen and Rotbart, 2013). Existing malware is effective against outdated systems installed in OT networks that suffer from a lack of cybersecurity controls and lack of additional cyber protection such as endpoint cybersecurity protection (antivirus software) (Stouffer et al., 2015).

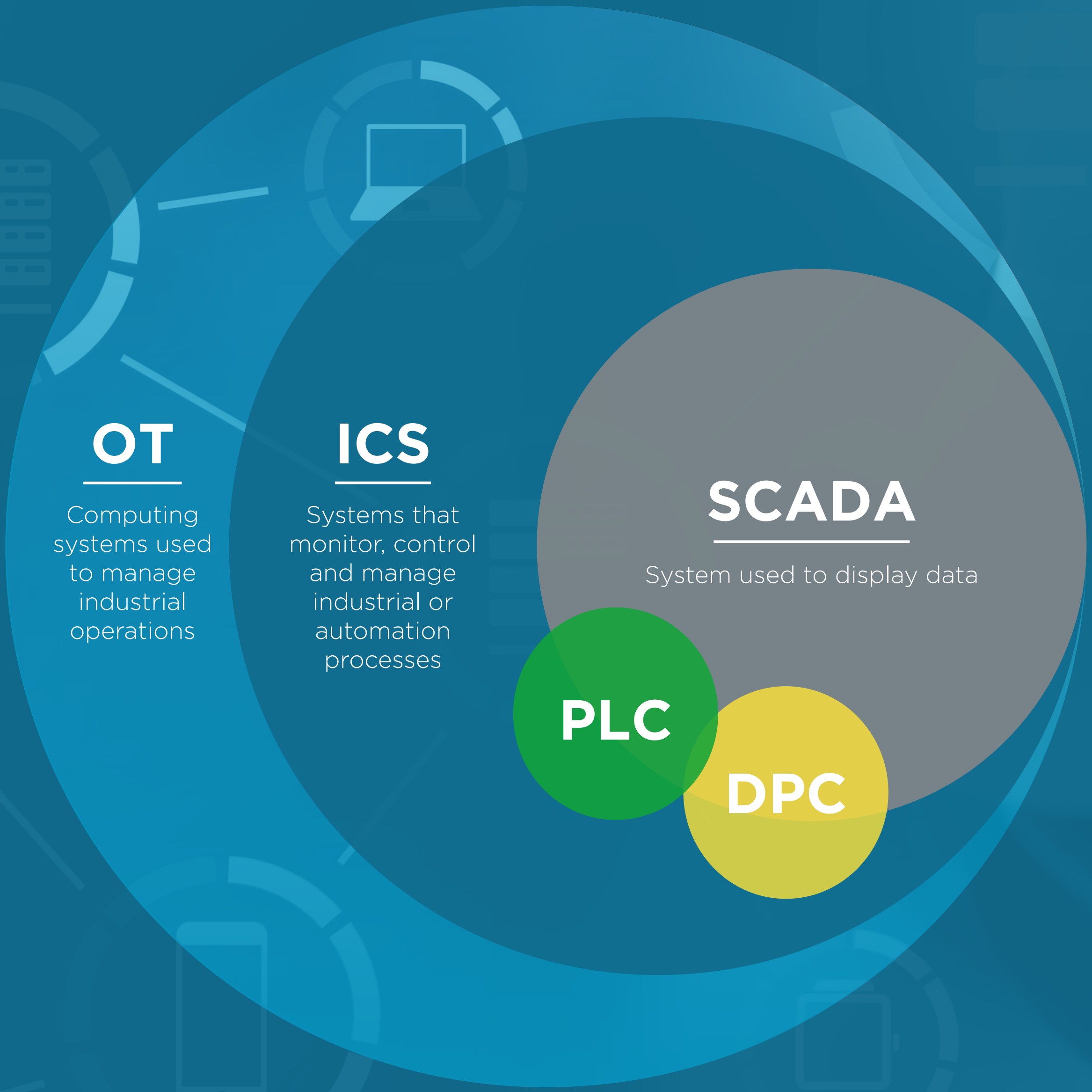
Attacks against systems that control and monitor critical civilian infrastructure are ranked high on the severity scale of cyberattacks. Among the most serious are attacks that endanger civilian lives, including water pollution or environmental damage due to sewage or chemical spills, also known as sanitary sewer overflows (SSO). Recent years have also seen a significant increase in cyberattacks on CI from a variety of actors, including states, terrorists, anarchists, competing commercial entities, criminals, organization insiders who act maliciously or inadvertently, and others (Bigelow and Lutkevich, 2021). Attacks on organizations in CI sectors have increased dramatically, from fewer than 10 in 2013 to almost 400 in 2020 — a 3,900 percent change (Thielemann et al., 2021).

Many organizations traditionally consider OT, which deals with machines and the physical world, as safe from cyberattack. Organizations often put great effort into strengthening their perimeter, but inadequately budget and invest in internal security, with an emphasis on OT system security. These investment discrepancies leave OT less guarded and open to attack. Once attackers have gained access to an organization’s systems, they can easily move and operate within them. Two cyberattacks in 2017 (NotPetya and WannaCry) demonstrated in practice that working according to this traditional model is no longer enough (Bigelow and Lutkevich, 2021).

The Relationship Between OT, ICS, and SCADA

It is important to differentiate between the role of OT, ICS, and SCADA. OT refers to computing systems used to manage industrial operations. SCADA is used to display data, and ICS, the systems that monitor, control and manage industrial or automation processes, is the level between OT and SCADA. Most ICS are considered continuous process control systems managed by PLC or discrete process control systems (DPC) that might use a PLC or some other batch process control device. Essentially, the OT tells the system "what to do," the ICS checks the systems' outcome ("how did you do?"), and SCADA processes data collected in the ICS and makes it accessible to users (Williamson, 2015). Figure 1 below illustrates it in this way.

Figure 1: Relationship Between OT, ICS, and SCADA

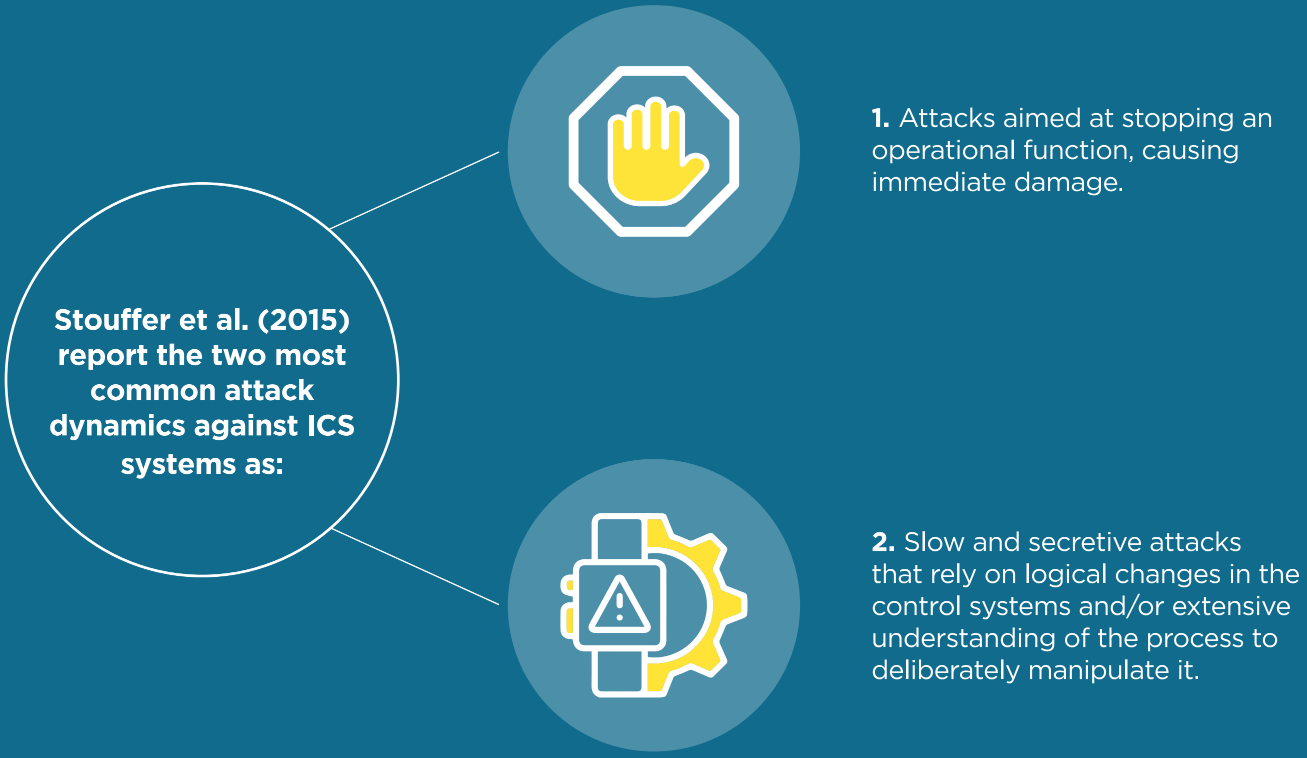

OT
Computing systems used to manage industrial operations
ICS
Systems that monitor, control and manage industrial or automation processes
SCADA
System used to display data
PLC
DPC

Source: Williamson (2015).

The Importance of Protecting ICS

ICS are crucial for industrial organizations since they assist in maintaining efficiency, evaluate data so that informed choices can be made, and identify faults in systems to help decrease downtime (Stouffer et al., 2015). ICS may be found in every operational facility and a variety of other entities, yet, despite their ubiquity, many remain vulnerable to cyberattacks.

Many communication protocols used in ICS are decades old and were not designed to address current cyber risks. Some ICS devices, protocols, and programs, for example, can be modified without authenticating the user, and some are exposed to the Internet. Furthermore, ICS were built to be fully independent of any other system for reasons of reliability. Nevertheless, cost and efficiency considerations push operators to connect ICS to industrial networks and even to the Internet, even though they were not intended for that environment, thus placing them at a higher risk for cyberattack, as they become exposed to the outer world, without proper security (Stouffer et al., 2015). According to the biannual risk and weakness report published by a cybersecurity company working in the ICS domain, awareness of the ICS security field rose as a result of high-profile cyberattacks on CI and industrial plants. Consequently, there has been a drastic increase in detecting security vulnerabilities in ICS, along with the rise of public and government awareness of ICS security. Out of the 637 ICS vulnerabilities affecting 76 vendors, published by Claroty in the first half of 2021, 65 percent have a high likelihood of causing a total loss of availability to the system (Claroty Team82, 2021).



Stouffer et al. (2015) report the two most common attack dynamics against ICS systems as:

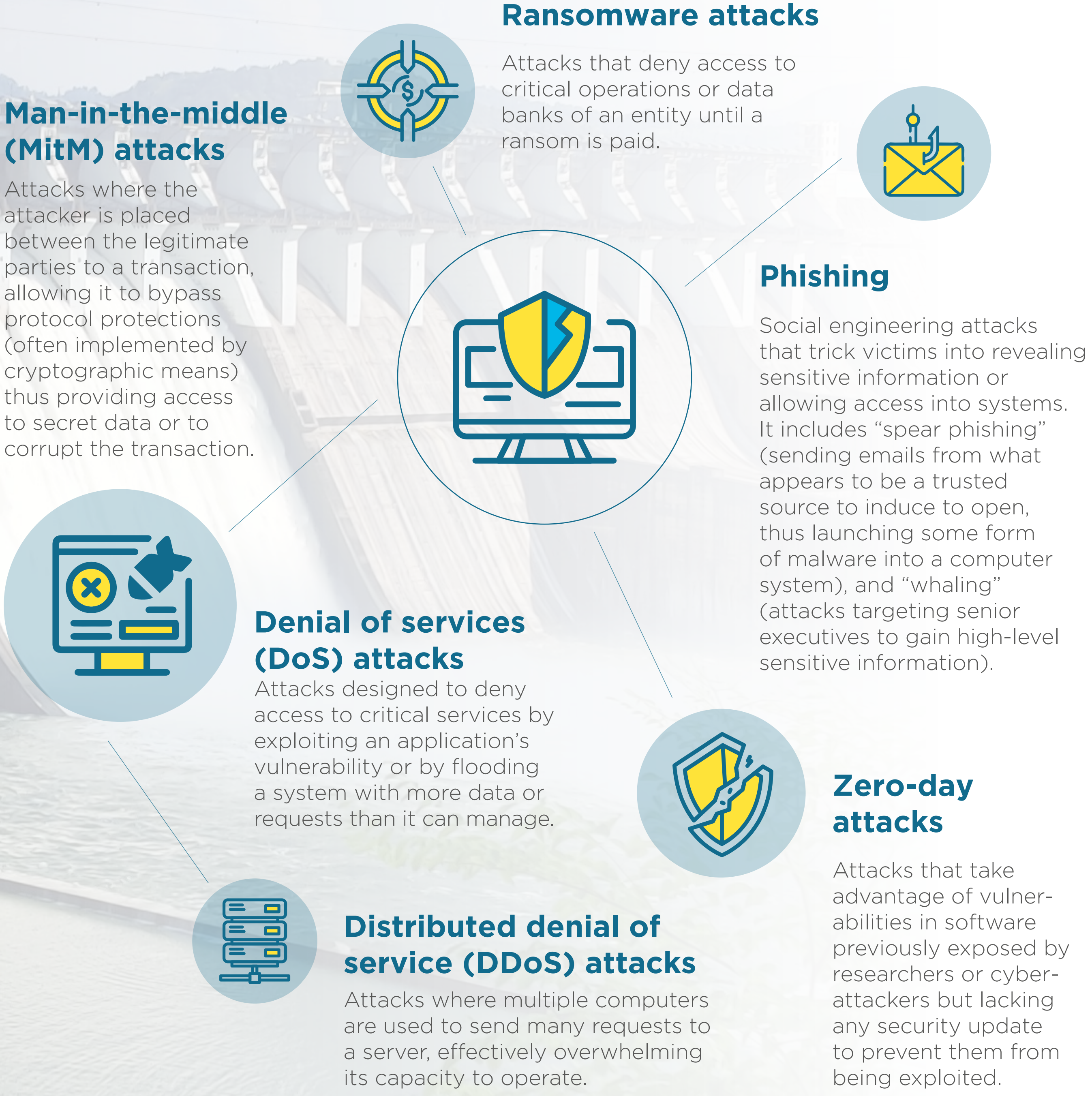
1. Attacks aimed at stopping an operational function, causing immediate damage.

2. Slow and secretive attacks that rely on logical changes in the control systems and/or extensive understanding of the process to deliberately manipulate it.

Types of Cyberattacks

In cyberspace, the human factor is responsible for most failures and malfunctions. In 2017, approximately 52 percent of US business owners acknowledged the risk of a cyberattack due to the human factor, resulting from act or omission on the part of an organization's employees (Kaspersky, 2017b). Figure 2 below provides a brief description of several types of cyberattacks.

Figure 2: Types of Cyberattacks



Ransomware attacks

Attacks that deny access to critical operations or data banks of an entity until a ransom is paid.

Man-in-the-middle (MitM) attacks

Attacks where the attacker is placed between the legitimate parties to a transaction, allowing it to bypass protocol protections (often implemented by cryptographic means) thus providing access to secret data or to corrupt the transaction.

Phishing

Social engineering attacks that trick victims into revealing sensitive information or allowing access into systems. It includes "spear phishing" (sending emails from what appears to be a trusted source to induce to open, thus launching some form of malware into a computer system), and "whaling" (attacks targeting senior executives to gain high-level sensitive information).

Denial of services (DoS) attacks

Attacks designed to deny access to critical services by exploiting an application's vulnerability or by flooding a system with more data or requests than it can manage.

Zero-day attacks

Attacks that take advantage of vulnerabilities in software previously exposed by researchers or cyberattackers but lacking any security update to prevent them from being exploited.

Distributed denial of service (DDoS) attacks

Attacks where multiple computers are used to send many requests to a server, effectively overwhelming its capacity to operate.

Source: Authors - adapted from Check Point Software (n.d.).

Threat Actors

The Canadian Centre for Cyber Security (2018) reports that various threat actors might have an interest in disrupting the proper function of water infrastructure because of ideological, economic, political, personal, or other interests. Table 1 below lists the main types of threat actors.

Table 1: List of Threat Actors

Nation-state actors

Sovereign states attack numerous targets in cyberspace causing varied effects, from website defacement to extensive damage to infrastructure. Their goal is usually geopolitical.

Cybercriminals (Financially motivated threat actors)

One of the most common motives for cybercriminals is profit. They tend to target weakly protected organizations, which are vulnerable to disruption and have an ability to pay, or whose valuable assets such as data, intellectual property or funds can be stolen online.

State-sponsored attackers and advanced persistent threat (APT) groups

APT groups are very technically capable threat actors. Some APTs are state-sponsored, but maintain plausible deniability as they are usually not overtly part of a government. APT groups pursue countries' strategic goals and can use advanced capabilities in a sustained manner to attack large, possibly better protected entities. Their targets may include state institutions, CI, and companies possessing key assets. The common objective for these attackers is achieving a strategic goal for their sponsor, in the form of disruption or obtaining sensitive information. Recent examples include the SolarWinds cyberattack which exploited vulnerabilities in the software supply chain.

Terrorists

These actors are interested in realizing their ideology by using violence towards the civilian population. Terrorists sometimes use unsophisticated approaches, applying widely available tools that require little technical skill to deploy.

Internal threats actors

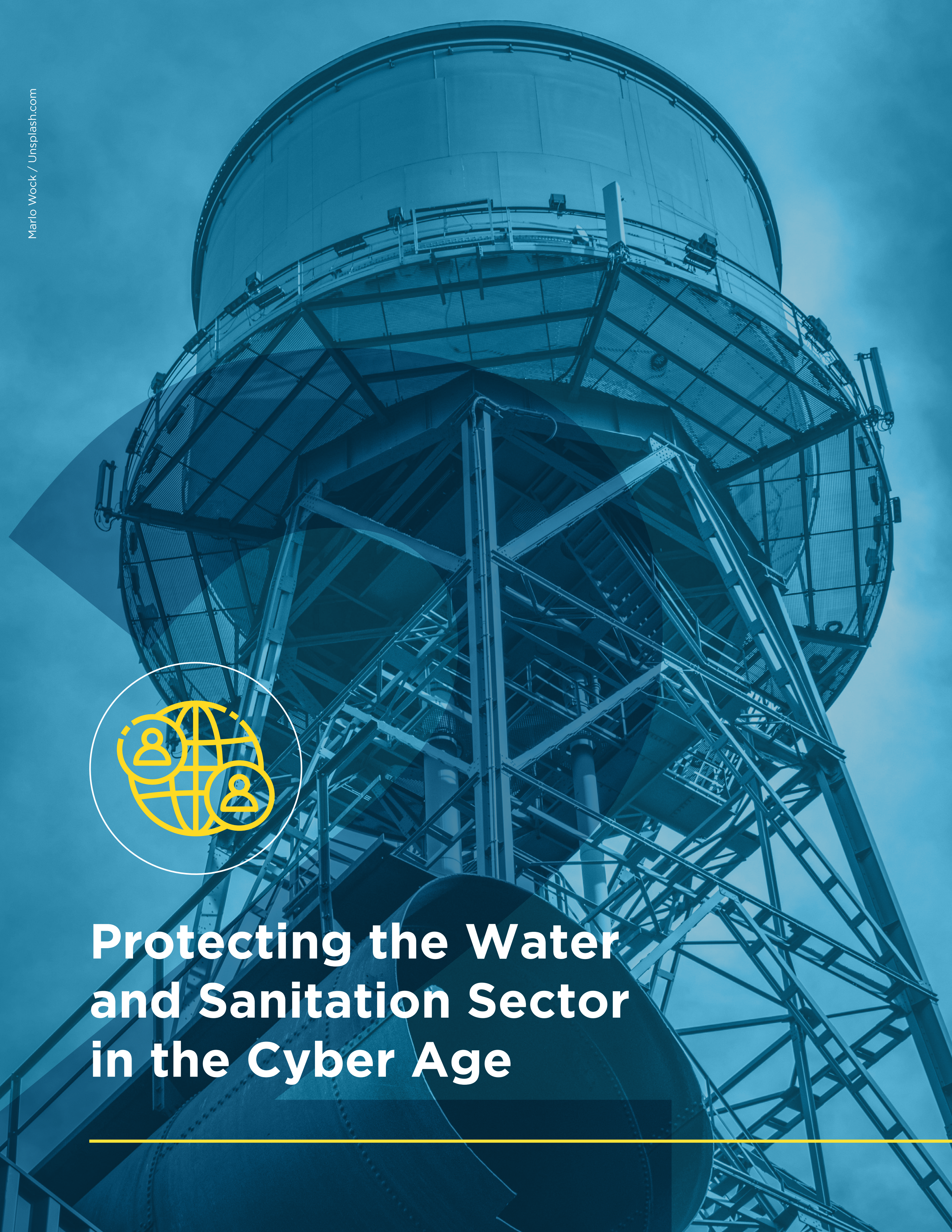
Any current or former employees, suppliers, or contractors of an organization, who have legitimate access to its systems and facilities, may represent a potential cyberthreat. These individuals may have extensive knowledge of the organization's systems and security controls. Those who decide to use their knowledge against their organization are usually driven by revenge (categorized as disgruntled employees), psychological, ideological or financial reasons. They typically want to damage the organization's reputation or steal confidential information such as intellectual property.

Hacktivists

Individuals or groups such as Anonymous that use hacking to promote their social or ideological goals. In most cases, their main objective is to raise awareness for the cause rather than to specifically cause damage to CI.

Source: Authors – adapted from Flashpoint (2021).

In LAC, the prominent threats are usually financially motivated, such as attacks by FIN11 and UNC2053 (two well-established financial crime groups), and often take the form of ransomware and malware attacks. According to Mandiant, advertisements for data stolen from LAC organizations during ransomware incidents increased 550 percent in just one year (from 2020 to 2021). This activity affected several countries, most frequently Brazil, Colombia, and Mexico, and involved industrial facilities, including energy providers and other utilities (Caparros, 2022).



Marlo Wock / Unsplash.com

Protecting the Water and Sanitation Sector in the Cyber Age

The Importance of Protecting Critical Infrastructure

As described in Chapter 1, CI is defined as such by the impact of its failure, which could trigger a substantial crisis. It is important to plan and implement CI protections strategically considering a series of predictions we describe more fully in this section.

Predictions About Cybersecurity of CI as Premises for Strategic Planning

While the following predictors may not fully apply to LAC, they do provide a general starting point for strategic planning.

By 2024, a cyberattack will damage CI, in a way that a member of the G20 will reciprocate with a declared physical attack. Also, 80 percent of CI organizations will abandon their existing siloed security solution providers, in order to bridge cyber-physical and IT risks by adopting hyper-converged solutions (Snow, 2022).

By 2025, attackers will have weaponized a CI cyber-physical system (CPS) to intentionally and successfully harm or kill humans (Moore, 2021a).

Through 2025, 30 percent of CI organizations will experience a security breach that will result in the halting of operations or a mission critical CPS (Moore, 2021b).

Through 2026, less than 30 percent of US CI owners and operators will meet newly mandated government security requirements for CPS (Snow, 2022).

Infrastructure Interdependencies and Security

The growing use of IT together with the free market's increasing reliance on infrastructure-provided products and services enhances the prevalence of infrastructure interdependency and the significance of the phenomenon whereby damage done to one infrastructure system affects another. Disruption of one infrastructure system can have a significant impact on the ability of other infrastructures to operate, and in many cases, can result in the collapse of other infrastructures connected to the affected infrastructure (Baram and Menashri, 2015). This is why US CI is often referred to as a "system of systems" (Stouffer et al., 2015).

The ability to identify and analyze interdependencies is clearly an important part of protecting CI. Although interdependencies are a common feature of CI systems, and often materialize via digital connections through information and communication technology, most are regionally determined, that is, they are closely related to geographic proximity and integrated regional networks. This is particularly true, for example, in the Baltic Sea Region and especially in Nordic countries, where CI in many sectors form part of the very same Nordic infrastructure system (Pursiainen et al., 2007).

Actors involved in infrastructure cyber protection must study and examine the connections and dependencies between the various infrastructures, create redundancies, and design systems to be resilient to ripple effects (the so-called "Domino Effects") impacting other heavily reliant infrastructures in the event of loss or damage to one of them (Menashri and Baram, 2015). When performing vulnerability assessments, establishing response and recovery plans, and managing other security and protection concerns, water and wastewater systems have distinct interdependencies with other infrastructures that must be considered (Gillette et al., 2002).

Aleksei Zaitcev / Unsplash.com

Examples of Infrastructure Interdependencies

According to a model suggested by Steven Rinaldi in a study conducted with other researchers (Rinaldi, Peerenboom and Kelly, 2001), four types of interdependencies can be identified:

Physical Interdependency: when one system is dependent on the physical output of another system(s).

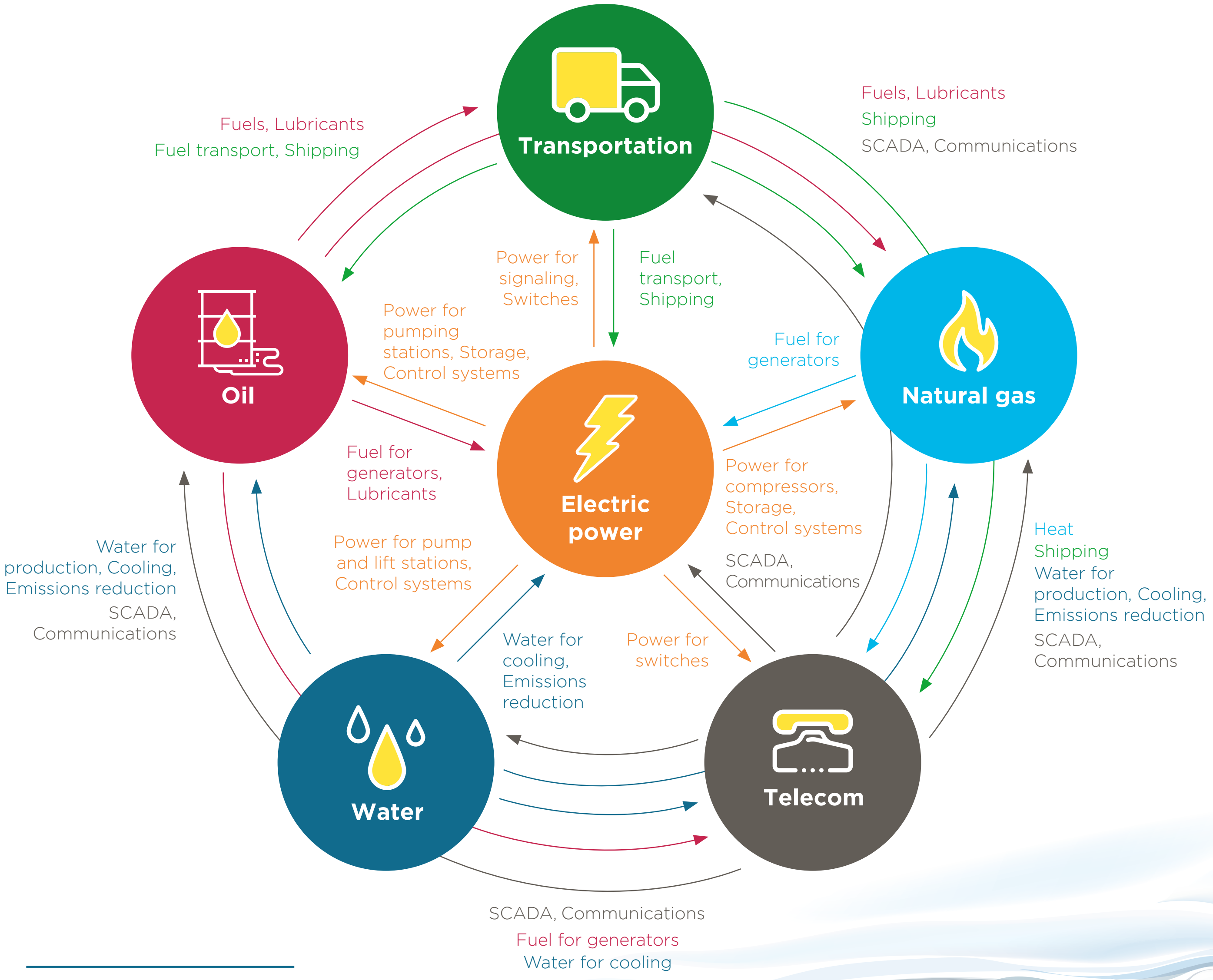
Geographic Interdependency: when a system(s) can be affected by a change in the proximal close environment.

Cyber Interdependency: when systems are communicating through cyberspace.

Logical Interdependency: when systems are dependent on one another in any other form of interdependence, not already specified.

The model included as Figure 3 below provides a visual image of the interdependencies described above.

Figure 3: Infrastructure Interdependencies Model

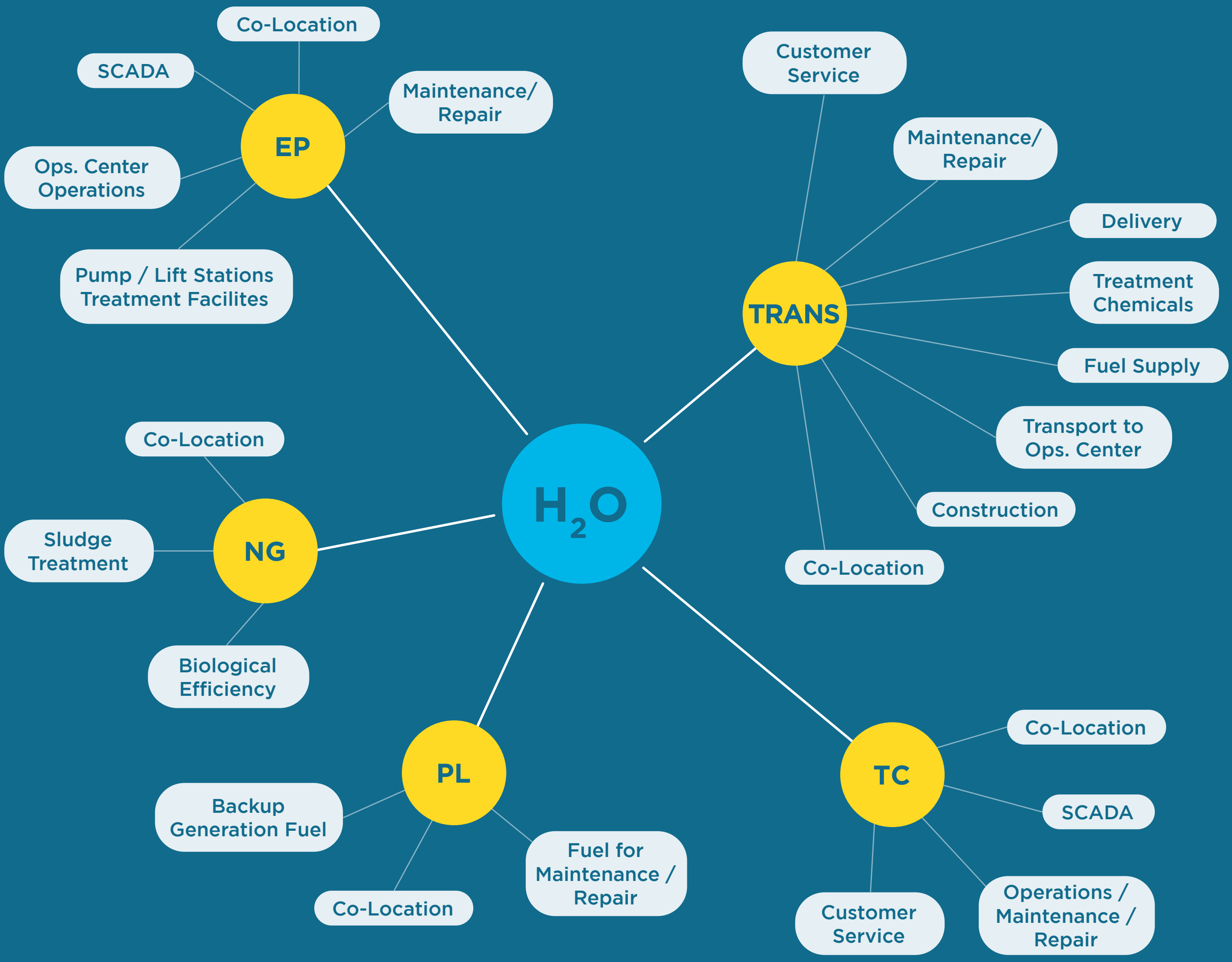

Transportation
Oil
Natural gas
Electric power
Water
Telecom
Fuels, Lubricants
Fuel transport, Shipping
Fuels, Lubricants
Shipping
SCADA, Communications
Power for signaling, Switches
Fuel transport, Shipping
Power for pumping stations, Storage, Control systems
Fuel for generators
Fuel for generators, Lubricants
Power for compressors, Storage, Control systems
SCADA, Communications
Water for production, Cooling, Emissions reduction
SCADA, Communications
Power for pump and lift stations, Control systems
Water for cooling, Emissions reduction
Power for switches
Heat
Shipping
Water for production, Cooling, Emissions reduction
SCADA, Communications
SCADA, Communications
Fuel for generators
Water for cooling

Source: Rinaldi, Peerenboom and Kelly (2001).

Water and Wastewater Interdependencies

When studying cyber vulnerabilities and designing their respective cybersecurity protection, the specific interdependence of wastewater and water infrastructure must be examined, as these infrastructures are linked to the major clean water suppliers for a country or region (Gillette et al., 2002). As an example, we can look at the 2009 Cinchona earthquake in Costa Rica, which caused heavy landslides and mud flows that resulted in damage to water and sewage systems and had significant impacts on the availability of clean water. It shows how natural disasters can influence wastewater facilities, and as a result, affect the availability of clean water (Deubelli, 2019). Figure 4 below illustrates infrastructure dependencies, including their dependencies on other types of infrastructures (transportation, gas, etc.).

Figure 4: Infrastructure Dependencies



Notes: **H_2O – the W&S sector, EP – electric power, NG – natural gas, PL – petroleum liquids, TRANS- transportation, TC – telecommunication.**

Source: Gillette et al. (2002).

Based on interviews conducted during this study, we learned that in most countries, including those in LAC, water and wastewater infrastructure is old and not as efficient as it can be. Therefore, the industry must undergo digital transformation to expand access to clean water and ensure continued access to it. Digitalization is improving utility operations by increasing their efficiency, upgrading services, and updating their technologies. In addition to expanding service coverage to more people, digitalization has financial benefits: companies that have higher digital maturity report 30 percent more revenue growth compared to lower maturity companies (Deloitte Insights, 2020).

As the W&S sector becomes more digitalized, it also becomes increasingly vulnerable to cyberattacks. A lack of awareness of cyber risks, resulting in a lack of investments in their mitigation, increases their potential damage. As proposed by Mirjana et al. (2020), cybersecurity in the industrial sector, which depends on IIoT technologies and is vulnerable to specialized cyberattacks, should be managed using adequate frameworks, which will strengthen the cyber-resiliency of these infrastructures.

Cybersecurity in the Water and Sanitation Sector

Industry 4.0 and the Paradox of Hyperconnectivity

Industry 4.0 refers to the fourth industrial revolution, in which the industrial sector becomes more digitalized and automated, and adopts new technologies in industrial processes, such as AI, Big Data, blockchain, drones, and virtual and augmented reality (VR/AR). The W&S sector is transforming towards the Industry 4.0 vision, which will introduce entirely new challenges due to the complex hyperconnectivity and increased range of threats. Incorporating IoT devices introduces concerns about data loss, information theft, privacy, weakened network protection, and more. As additional devices are being connected to operational networks, utilities face increased vulnerability and hackers have more opportunities to access networks as use additional attack vectors.

Remote metering solutions (smart metering) are a clear example of the sector's evolution towards Industry 4.0. The evolution of communication technologies means that systems are operated remotely and managed centrally. Thanks to more frequent and higher quality data capture, companies can offer new and enhanced services to clients, such as proactively communicating issues, warning regarding unusual water consumption, and recommendations for responsible water consumption. In addition to qualitative improvements in direct citizen services, remote metering offers the possibility for enhanced smart network management, early detection of leaks, enhanced energy efficiency, and ultimately, optimization of processes and efficient integrated water cycle management (Mirjana et al., 2020).

Why Is Industry 4.0 Important for the W&S Sector?

Mirjana et al. (2020) states that in the W&S sector, Industry 4.0 is particularly important for the reasons highlighted in Table 2.

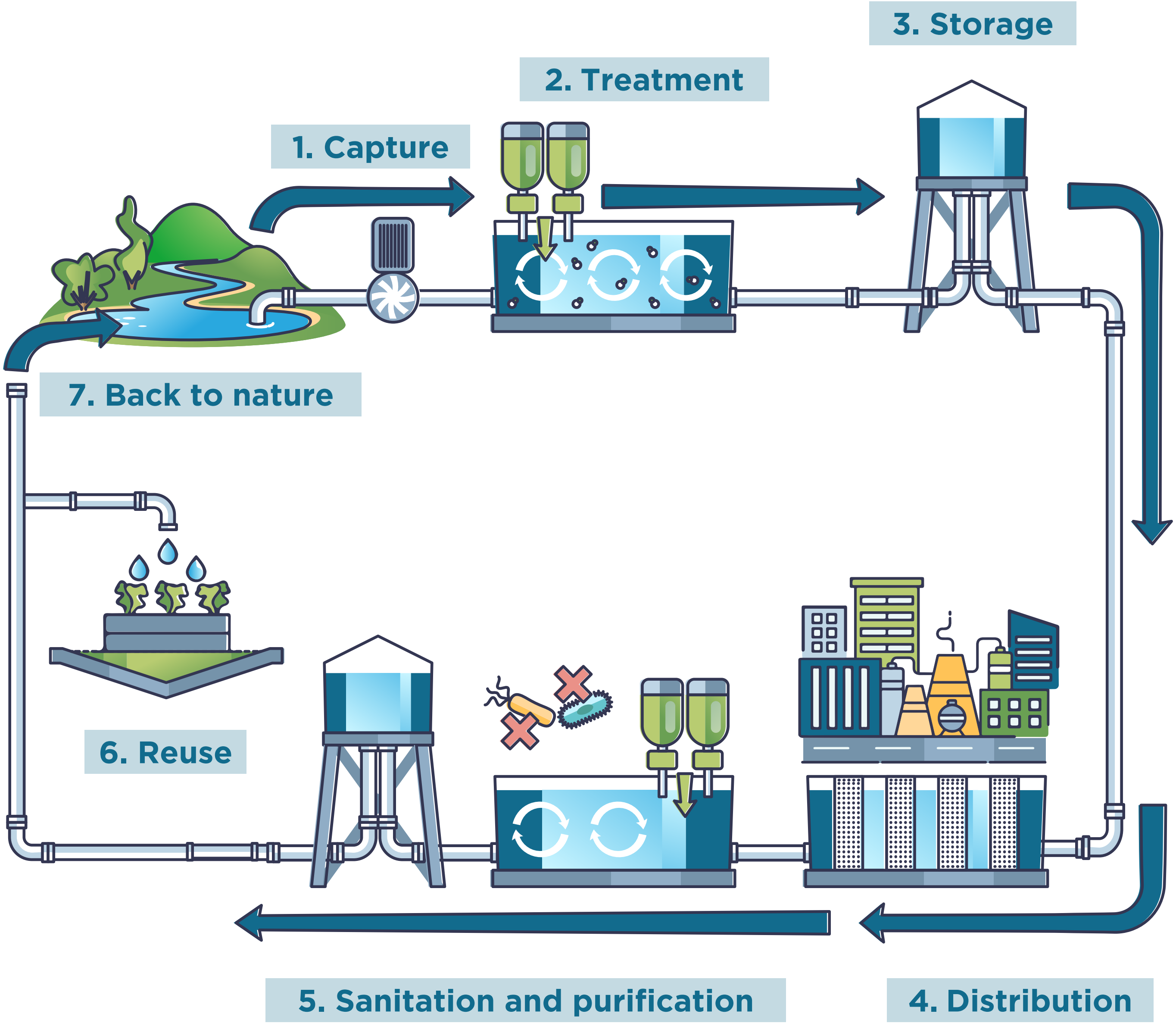
Table 2: Why Industry 4.0 Is Important for the W&S Sector

Factors	Description
Aging Workforce	The water industry is experiencing a generational change in its workforce. Many people are approaching retirement, retiring or leaving the sector for better opportunities. Their departure depletes the workforce, but more disconcerting is the loss of their undocumented knowledge and experience. Due to declining revenues, tight budgets, and technological immaturity, many of the best and brightest are not attracted to the water industry so open positions might either be filled with suboptimal resources or left unfilled.
Asset Management	The assets at many water utilities are old and in need of rehabilitation or replacement. Capital budgets are expected to decline over the next several years. Operating costs are skyrocketing as assets frequently break down and require emergency repairs. In addition, asset management practices are outdated compared to industries like oil and gas, chemicals, and electrical utilities.
Climate Risk	The first three industrial revolutions transformed modern society with the steam engine, the age of science and mass production, and the rise of digital technology, fundamentally changing the world. Consequently, the planet and its climate also changed. As a result, risks are increasing for the environmental, economic, and social aspects of human civilization, challenging society to find new ways to live that are more resilient and sustainable. Water utilities and the communities they serve are challenged with dwindling water supplies, more frequent and intense rainfall events that exacerbate combined sewer overflows (CSO) and sanitary sewer overflows (SSO), and rising sea levels and salt-water intrusion.
Emerging Contaminants	Microplastics, pharmaceutical compounds, and other refractory compounds have been detected in drinking water sources, sewage, wastewater sludge, and biosolids. These contaminants are harmful to humans and aquatic life. The US EPA and its state environmental agencies will soon require water utilities to actively monitor and treat these contaminants according to pending regulatory limits.
Societal issues	These include such things as population growth and migration, both domestically from the countryside to cities, and internationally.

Source: Mirjana et al. (2020).

Industry 4.0 is required for the evolution of the W&S sector and its increased efficiency. Moving to Industry 4.0 requires using new digitalized technologies in water infrastructure, which exposes it more than ever before to cyberattacks. Figure 5 offers an illustration of the various stages in water treatment.

Figure 5: Stages in Water Treatment



Source: Aqualia Group (2019).

The Impact of Cyberattacks on Water Infrastructure

The provision of water and wastewater services has long been considered a critical component of economic development. Water is an essential resource for the survival of people and the planet. Disruptions to water production, transmission and distribution systems can result in disease and morbidity, damage agriculture and industry, threaten citizens' water security, and even undermine national resilience. Therefore, water suppliers must always ensure a stable and constant water supply to minimize potential damage to citizens' quality of life (Daigger et al., 2019).

The CIA Triad of Data Security

The confidentiality, integrity, and availability triad, abbreviated CIA, was created to guide organizations' digital security policies around the major cyber risks. Confidentiality limits access to restricted systems or data to authorized users only. Integrity assures the trustworthiness, accuracy, and completeness of the systems, processes or data. Availability guarantees reliable access to the systems or data (Wesley, 2023). In many IT contexts, confidentiality may be generally more important than its integrity, which may be more important than its availability. However, in ICS-centered environments, this order of importance is often reversed (Weiss, 2008): Extremely high system and service availability may be more important than their integrity, with confidentiality being relatively less important as ICS contexts usually deal with less sensitive data.

To illustrate the basic principles of information security outlined by the CIA Triad, examples of risks to infrastructure systems could include (Weiss, 2008):

1. Impairment of critical system availability, e.g., the ability to use the critical computerized system as specified at any time, and from any place designated for this purpose.
2. Impairment of critical system production capacity.
3. Impairment of the reliability and integrity of critical systems information or processes, with results contrary to the systems' intended purpose. Unauthorized alteration or destruction of information may impair the proper functioning of critical computerized systems.
4. Breach of the confidentiality of information stored in these systems could affect critical computerized systems or the organization's information assets. One example may be the disclosure of data used by commercial divisions within utilities.

Key Elements That Can Improve the Sector’s Cybersecurity Posture

According to the State of the Sector Cybersecurity Report for 2021, published by the US Water Sector Coordinating Council (WSCC, 2021), the top four areas of concern affecting cybersecurity for the W&S sector are gaps in:

Sector-specific training and education

Technical assistance, conducting assessments, and the availability of tools

Cybersecurity threat information

Funding, such as that obtained through government loans and grants or through public-private partnership funding

A US Department of Energy publication (Clark et al., 2017) reveals the top five technical areas in the W&S sector that suffer from frequent security gaps:

1. Network configurations
2. Protection of media and streaming platforms
3. Remote access to water operational systems
4. Documented policies and procedures
5. Inadequately trained staff

A survey conducted by the WSCC (2021) on the state of cybersecurity for water infrastructure in the US identified needs for the sector, ranked from most to least needed:

1. Technical assistance
2. Federal grants or loans for cybersecurity equipment or services
3. Training and education targeting the sector
4. Assurance of supply chain integrity for IT and OT hardware and software
5. Funding to hire cybersecurity personnel
6. Cyber security threat information

Rob Bates / Unsplash.com

According to a survey conducted by the Water Information and Sharing Analysis Center (WaterISAC, 2021) on the state of water infrastructure cybersecurity in the United States, what follows is a representative sampling across all size systems and provides the following 2021 budget allocations for cybersecurity:

- **38%** of systems allocate less than 1% of budget to IT cybersecurity
- **22.1%** of systems allocate 1–5% of budget to IT cybersecurity
- **6.3%** of systems allocate 6–10% of budget to IT cybersecurity
- **4.1%** of systems allocate more than 10% of budget to IT cybersecurity
- **44.8%** of systems allocate less than 1% of budget to OT cybersecurity
- **20.95%** of systems allocate 1–5% of budget to OT cybersecurity
- **4.9%** of systems allocate 6–10% of budget to OT cybersecurity
- **1.7%** of systems allocate more than 10% of budget to OT cybersecurity

Patrick Federi / Unsplash.com

The figures above analyze reports of budget allocations in practice. As such, they do not necessarily indicate an optimal allocation of cybersecurity budget. In fact, they may document the insufficient budget allocated to mitigate cyber risks in critical utilities, and specifically, in the OT domain.

Potential Damage and Its Impact on Water Infrastructure

The potential impact on drinking water production or wastewater treatment may include the following scenarios (Thielemann et al., 2021):

Citizens would be deprived of safe drinking water and sanitation

Hospitals would not be able to operate

Fire hoses would not work

Schools, offices, and government facilities would be closed

Agricultural crops would be damaged

Several manufacturing segments would be halted

Water supply would be interrupted to nuclear facilities that rely on water cooling

All systems dealing with water supply, water quality, flood risk reduction, electricity, agricultural production, and wastewater are potentially vulnerable to cyberattacks, with devastating consequences for health, the environment, and the economy (Mission of Israel to the UN, 2021). Table 3 below presents possible scenarios in which cyberthreats to water facilities engaged in production, transmission, and purification may produce significant damage (OECD Water, n.d.).

Table 3: Potential Damage Scenarios

Potential damage	Area(s) of impact	Scenario #1	Scenario #2
Impairment of the functional flow of water production and transmission	• Urban and domestic use • Industrial productivity • Agricultural productivity • Human health	(a) A high-pressure water jet can cause various stones and objects that are above and around the damaged pipe to fly around, potentially harming individuals and the environment.	(b) Leakage from an underground water pipe causes sand drift, which can lead to damage to foundations, nearby underground infrastructure, roads, and buildings, causing them to collapse and flood.
Water source contamination	• General public	Manipulation of the water purification or desalination process.	CSO or SSO causing massive well water contamination.
Environmental and ecological damage from sewage treatment	• Agricultural productivity • Human health • Environment	Sewer lines are under internal hydraulic pressure (drain lines) and when damaged, can cause harm to water lines. Usually, the flow in sewer lines relies on gravity. Therefore, the main risks from pipe damage are environmental pollution, contamination of underground water sources, and harmful health effects.	CSO or SSO causing a massive well water contamination and environmental issues.

Source: Authors and OECD Water (n.d.). Scenarios (a) and (b) were taken from Ali and Choi (2019).

Harry Shelton / Unsplash.com

Water and Sanitation Sector Preparedness in Latin America and the Caribbean

Regional Cybersecurity in LAC

Regional Trends

Countries differ in their approach to cybersecurity, depending on their economic, political, and cultural landscape. Some countries view cybersecurity as a national security issue, while others view it as an economic development challenge. As mentioned in the IDB and OAS 2020 cybersecurity report, the LAC region is not sufficiently prepared to handle cyberattacks. Only seven of the thirty-two countries have a CI protection plan, while twenty have established cybersecurity incident response teams. This limits their ability to identify and respond to attacks.

The Cybersecurity Capacity Maturity Model for Nations (CMM), developed by the Global Cyber Security Capacity Centre at the University of Oxford (2021), is a methodical framework designed to review a country's cybersecurity capacity. The CMM follows a comprehensive approach that evaluates nations' maturity in five dimensions:

1. Cybersecurity policy and strategy
2. Cyber culture and society
3. Cybersecurity education, training, and skills
4. Legal and regulatory frameworks
5. Standards, organizations, and technologies

CMM was used by the IDB and OAS in 2016 and 2020 to evaluate the maturity of LAC countries (IDB and OAS, 2016 and 2020). According to these evaluations, LAC countries made progress in their cybersecurity posture: some of the countries achieved higher levels of maturity in the Identification, Organization and Risk Management and Response indicators of the Critical Infrastructure Protection aspect, among other relevant improvements. The main trend seen in the region is the establishment of CI protection plans. In 2016, only one out of five countries had a cybersecurity strategy or a CI protection plan. By 2020, 12 countries in the region had approved national cybersecurity strategies, 7 countries had CI protection plans, while others were improving their capabilities at that time.

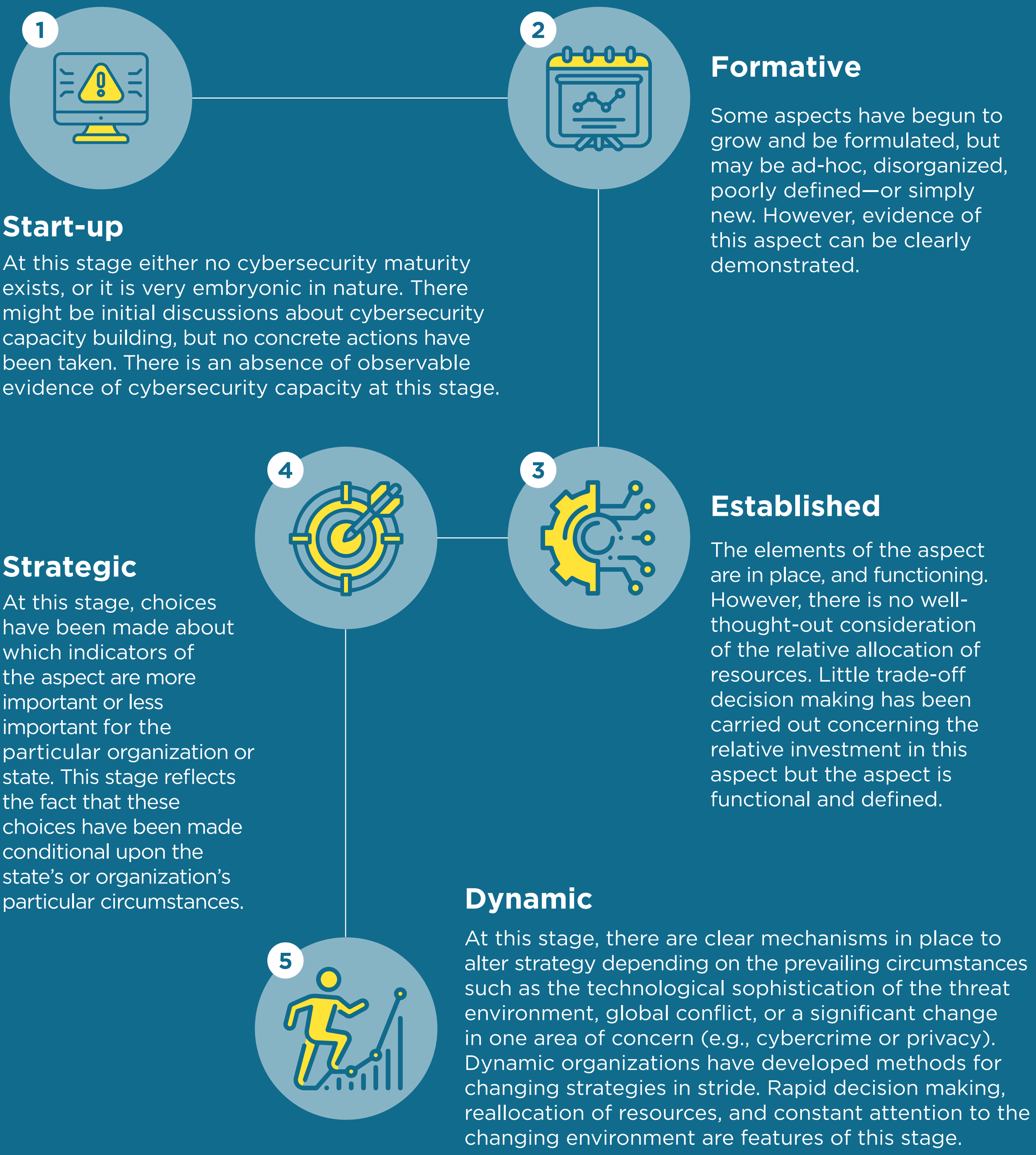
There has been a dramatic increase in the cost of global cybercrime. As reported by McAfee in its publication “The hidden cost of cybercrime” (Lewis, 2020), costs increased more than 50 percent from 2018–2020, going from USD 600 billion to over USD 1 trillion. A 2021 report issued by IBM security revealed that average cost per cyber incident in large companies in Latin America increased by 52.4 percent from 2020–2021, setting the average data breach cost at USD 2.56 million in LAC, while the average cost per incident globally was USD 4.24 million.

Argentina, Brazil, Colombia, and Mexico are among the bigger and more digitized economies in LAC. Consequently, these countries have some of the largest surfaces of exposure to cyberattacks, meaning they have more digital assets that may potentially be attacked. Encryption ransomware has become an important threat to CI in the region, where most of the attacked industrial automation systems were found to be in Brazil (0.9 percent), Mexico (0.5 percent), and Colombia (0.4 percent), with figures representing the percentage of computers attacked by malware in that same country. Fewer attacks were registered in Argentina, Chile, Costa Rica, Ecuador, Panama, Paraguay, and the Dominican Republic (Kaspersky, 2017a).

Critical Infrastructure Protection in the Region

The dimensions considered in the CMM seek to provide an assessment of the maturity level of a country’s cybersecurity capabilities, assigning a specific stage that corresponds to their degree of cybersecurity attainment. The five stages of maturity, which are assigned through an evaluation, range from the most basic (Start-up) to the most advanced (Dynamic).

Figure 6: The Five Stages of Maturity



1

Start-up

At this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.

2

Formative

Some aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined—or simply new. However, evidence of this aspect can be clearly demonstrated.

3

Established

The elements of the aspect are in place, and functioning. However, there is no well-thought-out consideration of the relative allocation of resources. Little trade-off decision making has been carried out concerning the relative investment in this aspect but the aspect is functional and defined.

4

Strategic

At this stage, choices have been made about which indicators of the aspect are more important or less important for the particular organization or state. This stage reflects the fact that these choices have been made conditional upon the state's or organization's particular circumstances.

5

Dynamic

At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict, or a significant change in one area of concern (e.g., cybercrime or privacy). Dynamic organizations have developed methods for changing strategies in stride. Rapid decision making, reallocation of resources, and constant attention to the changing environment are features of this stage.

Source: IDB and OAS (2020).

When this framework is applied to evaluate protection of CI in LAC countries, it is possible to assess the capacity of the individual governments to: **identify** its CI assets, engage in **organizational** efforts to regulate the cybersecurity of the aforementioned CI, and achieve competence in its **risk management and response**, recognizing each country's ability to secure its CI against cyberthreats.

Table 4 shows LAC country maturity in Critical Infrastructure Protection according to the 2020 study conducted by IDB and OAS.

Table 4: CMM Country Maturity in CI Protection for LAC

	Critical Infrastructure Protection														
Country	Identification					Organization					Risk Management and Response				
Antigua and Barbuda	■	2				■	2				1				
Argentina	■	2				■	2				■	2			
Bahamas	■	2				1					1				
Barbados	1					1					1				
Belize	1					■	2				1				
Bolivia	■	2				1					1				
Brazil	■	■	3			■	■	3			■	■	3		
Chile	■	2				■	2				■	2			
Colombia	■	■	3			■	■	■	4		■	■	■	4	
Costa Rica	1					1					1				
Dominica	1					1					1				
Dominican Republic	1					■	2				1				
Ecuador	1					1					■	2			
El Salvador	1					1					1				
Grenada	1					1					1				

	Critical Infrastructure Protection														
Country	Identification					Organization					Risk Management and Response				
Guatemala	1					1					1				
Guyana		2				1					1				
Haiti	1					1					1				
Honduras		2					2					2			
Jamaica		2				1					1				
Mexico		2					2					2			
Nicaragua	1					1					1				
Panama		2					2					2			
Paraguay	1					1					1				
Peru		2					2				1				
Saint Kitts and Nevis		2				1					1				
Saint Lucia	1					1					1				
Saint Vincent and the Grenadines	1					1					1				
Suriname	1					1					1				
Trinidad and Tobago		2					2					2			
Uruguay		2						3					3		
Venezuela	1					1						2			

Source: IDB and OAS (2020).

This study provides a critical vision of where LAC countries are individually, and the opportunities upon which the region as a whole can capitalize to improve its CI protection. Based on this information, we highlight that **the average maturity level of the region is still between 1 and 2** according to the CMM. In other words, most countries in LAC have just started formulating some cybersecurity initiatives involving their CI, with some of these strategies already in place. However, they are being implemented in an ad-hoc manner, lacking coordination among key stakeholders. In this regard, such risks associated with the lack of an institutionalized mechanism for facing CI vulnerabilities only exacerbate the region's internal response capacities, including Organization of Critical Infrastructure Protection, Crisis Management and Risk Management and Response—which, as a result, rank towards the bottom on average (IDB and OAS, 2020).

Why Is LAC More Vulnerable to Cyberattacks?

Along with other global regions, LAC has become increasingly digitalized. Over the last decade, LAC's Internet access has increased at an exponential rate (Prado, 2011). According to the International Telecommunication Union (ITU), more than two-thirds of LAC's population is now online, compared to only 53.6 percent of Internet users worldwide (ITU, 2019). The increase in Internet penetration of households occurred simultaneously with the growth in digitalization of companies, factories, and service providers, which required a more mature, comprehensive, and relevant cybersecurity strategy for the region.

When describing the LAC cybercrime threat landscape, one factor is especially important: the nexus between economic development, digitalization, governance, and crime. While LAC countries are incorporating global supply chains and continuing their economic development, institutional progress is catching up. The institutional fragilities in some countries result in impaired cybersecurity governance as in the lack of strong cybercrime legislation, proper cyber law enforcement, technical expertise, and international legal cooperation. This in turn could attract cybercriminals who believe the region to be an easy target (Pimenta Klein and Boguslavskiy, 2020).

Like other types of crime, the specific characteristics of cybercrime in LAC are mainly related to socio-economic vulnerability across the region. Given the availability of digital technologies that allow the easy conduct of cybercrimes, traditional crime groups decided to resort to cyber activities for potentially higher financial gains in a poorly regulated digital domain, resulting in lower risks for criminals.

In other words, cybercrime in LAC is defined by regional development fragilities, i.e., its rapid digitalization and adaptation to new technologies in the face of lagging regulation and policy. This vacuum of enforcement and authority created by expanding and evolving ICT use attracts malicious actors such as traditional crime groups. As a result, threat actors find numerous loopholes in both digital and social infrastructures and are thus motivated to engage in cybercrime activities in an almost unreserved manner (Pimenta Klein and Boguslavskiy, 2020).

Why Are There Not More Cyberattacks on Water Utilities in LAC?

As mentioned previously, water infrastructure in the LAC region is often old, and has not yet moved towards advanced technology systems. Infrastructure systems that are not digitalized or connected online are isolated from many cyber risks. However, two major points must be considered when talking about the number of cyberattacks on water utilities in the LAC region:

As the W&S sector moves toward more advanced technologies, the prediction is that we will see more cyberattacks on water utilities until proper cybersecurity mechanisms are put in place.

The lack of cyber-monitoring of already upgraded water utilities creates "blind spots" where cyberattacks we are not yet aware of could take place.

Regional Cooperation on Cybersecurity

For the last few decades, Latin America as a region has cooperated on cybersecurity issues and strengthened the capacity of countries in the region to counter digital threats. While such regional cooperation could foster cyber diplomacy convergence, countries in LAC have thus far not formed a regional bloc in conversations with the United Nations on the stability of cyberspace. Cybersecurity policies and protection mechanisms have been developed slowly by LAC countries ever since they were the first region to articulate a cybersecurity strategy in 2004 (Van Raemdonck, 2020).

The EU Institute for Security Studies (EUISS) identified the causes of this situation in the following factors:

1. Uneven levels of digital penetration
2. Little sense of urgency by policymakers in coordinating their cybersecurity responses due to a lack of public dissemination of high-profile attacks
3. Absence of financial resources to invest in national digital security
4. Lack of expertise on the part of policymakers and IT professionals

Other reasons for LAC's slow progress in adjusting to increasing cybersecurity threats are its limited awareness of cybersecurity measures and risks, a lack of trust between and within countries in the region, a disconnect between public and private sectors, and significant socio-economic disparities, meaning more people fall into crime, and within that, cybercrime. The EUISS recognizes that there are effective regional cooperation mechanisms that can help the region cope with digital threats. Multilateral organizations such as the IDB and OAS contribute to this effective cooperation through different programs, managed by their cybersecurity groups.

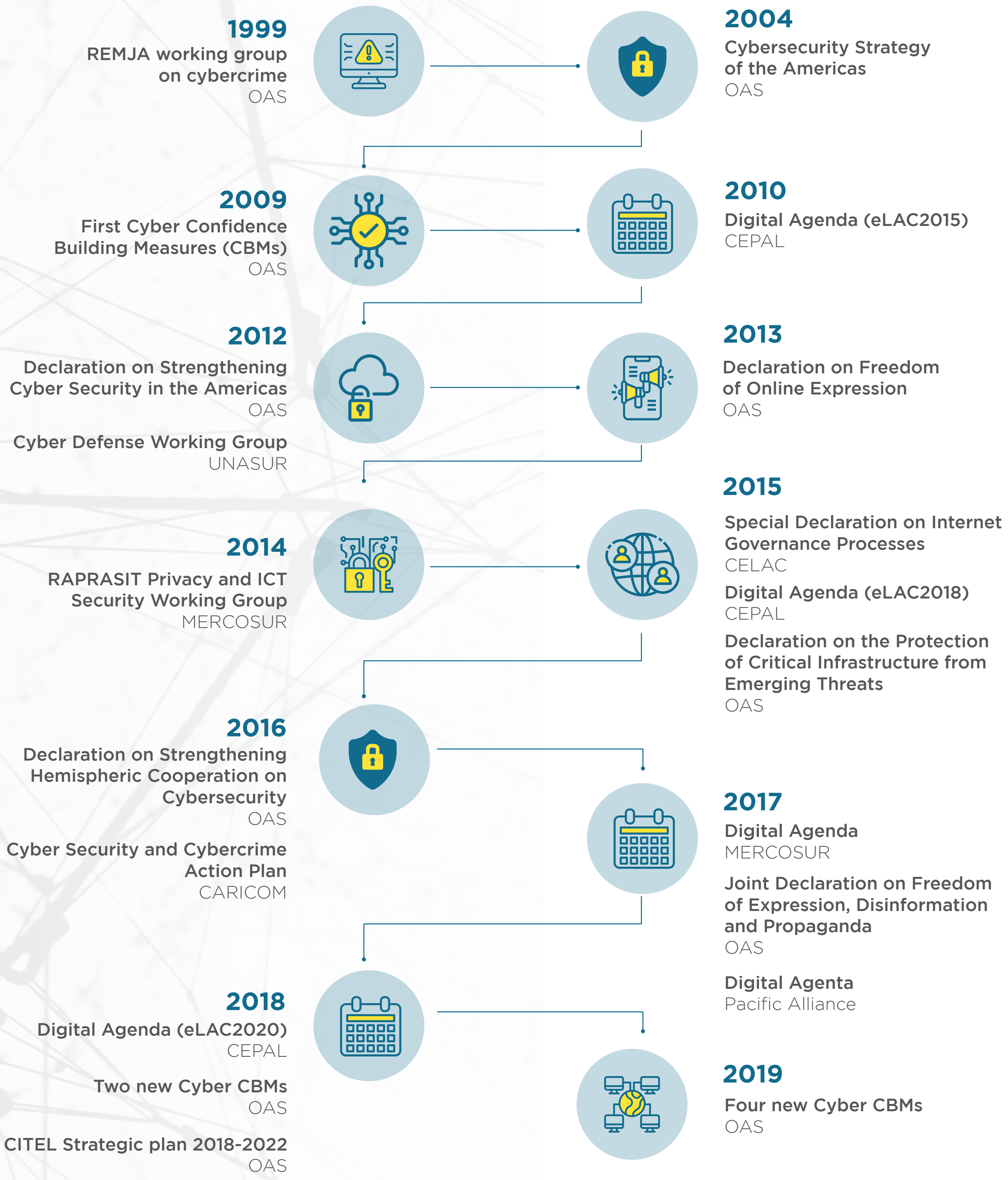
Cybersecurity developments in the private sector are taking place mainly thanks to the availability of financial, human, and technological resources. Therefore, cooperation between public and private sectors is needed. This could take the form of public-private partnerships (PPP) to promote cybersecurity policies at national, regional, and international levels. This kind of PPP requires good coordination and the decision-making authority to address cyberthreats.

Because cyberattacks can cross country borders, transnational cooperation is especially crucial in the cyber domain. Cyber policies should be updated and coordinated regionally, and countries should put efforts and resources towards this common field (Saavedra, 2015). Regional and sub-regional organizations such as the OAS, the Union of South American Nations (UNASUR), the Central American Integration System (SICA), and others can help harmonize strategies for the region's common cybersecurity, which will promote legislation and the cooperation of states in the region, as well as coherent operational plans (Saavedra, 2015).

Lack of Incentives

As the world's use of digital systems has experienced a sharp surge in recent years, the cyber defense crisis has escalated, and cyberattacks have increased dramatically. However, another explanation for the rise in the number of cyberattacks is that not enough resources have been invested to develop secure hardware and software products and services operating in cyberspace. For most companies, investing in their products' cybersecurity may not be financially viable as it may cost more than the potential damage to the companies from cybersecurity incidents involving their products. This in turn leads to few incentives for this type of investment (Brangetto and Kert-Saint Aubyn, 2015). A survey of owners and operators of CI conducted by the OAS and Microsoft in 2018 found that many governments in the region have neither established incentive programs to encourage such owners and operators to voluntarily adopt cybersecurity measures, nor begun to implement mandatory frameworks (OAS, 2018). The figure that follows provides an overview of 20 years of initiatives in the LAC region.

Figure 7: Cybersecurity Policy Initiatives in the LAC Region 1999–2019



1999
REMJA working group on cybercrime
OAS

2004
Cybersecurity Strategy of the Americas
OAS

2009
First Cyber Confidence Building Measures (CBMs)
OAS

2010
Digital Agenda (eLAC2015)
CEPAL

2012
Declaration on Strengthening Cyber Security in the Americas
OAS

Cyber Defense Working Group
UNASUR

2013
Declaration on Freedom of Online Expression
OAS

2014
RAPRASIT Privacy and ICT Security Working Group
MERCOSUR

2015
Special Declaration on Internet Governance Processes
CELAC

Digital Agenda (eLAC2018)
CEPAL

Declaration on the Protection of Critical Infrastructure from Emerging Threats
OAS

2016
Declaration on Strengthening Hemispheric Cooperation on Cybersecurity
OAS

Cyber Security and Cybercrime Action Plan
CARICOM

2017
Digital Agenda
MERCOSUR

Joint Declaration on Freedom of Expression, Disinformation and Propaganda
OAS

Digital Agenta
Pacific Alliance

2018
Digital Agenda (eLAC2020)
CEPAL

Two new Cyber CBMs
OAS

CITEL Strategic plan 2018-2022
OAS

2019
Four new Cyber CBMs
OAS

Source: Van Raemdonck (2020).
Notes: REMJA: Meeting of Ministers of Justices, other Ministers, Prosecutors and Attorney Generals of the Americas; CITEL: Inter-American Telecommunication Commission; RAPRASIT: Meeting of Authorities on Privacy and Information Security and Technological Infrastructure.

Interviews: Methodology and Insights

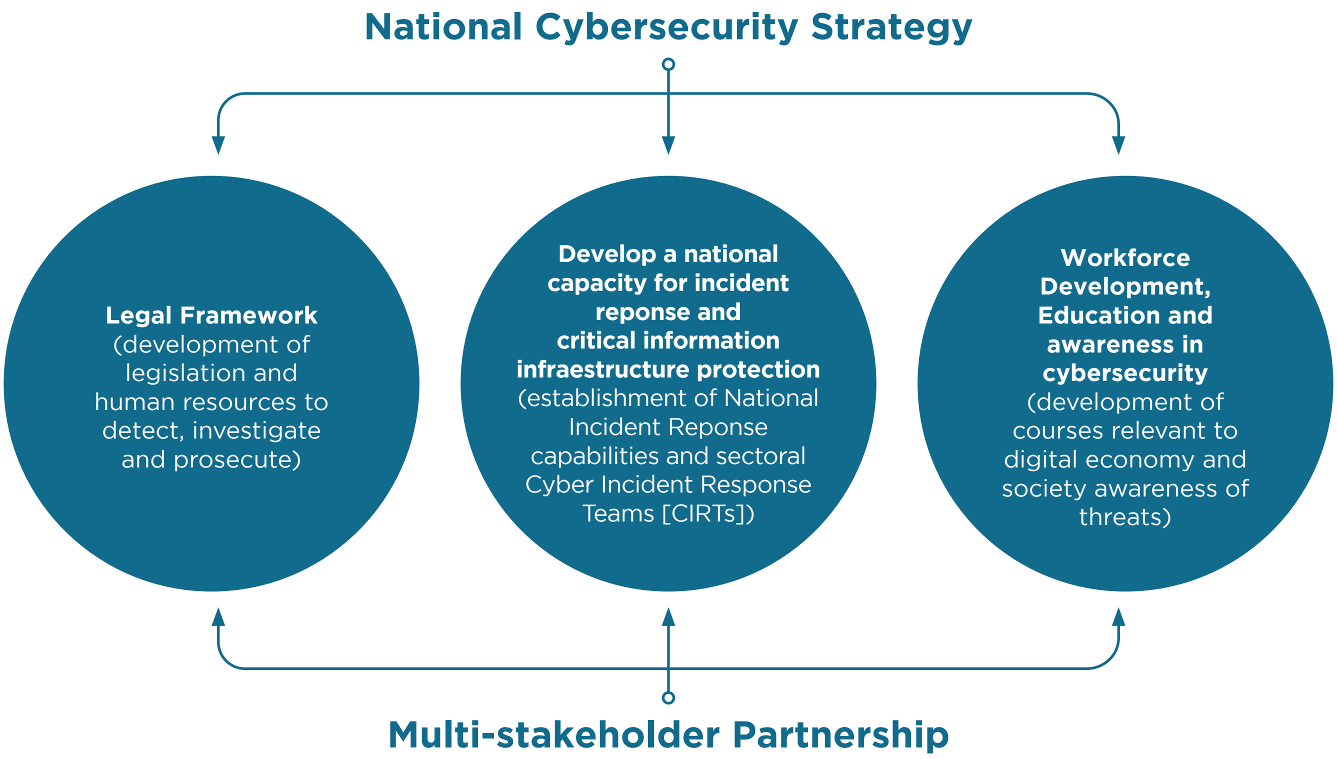
To further enhance our report, we conducted several interviews in the region. The interviews included representatives from institutions at the state level as well as water utilities in the following seven countries: Belize, Brazil, Chile, Jamaica, Panama, Suriname, and Trinidad and Tobago. Interviews were conducted through online video calls, and each interviewee was asked about cybersecurity in the region, in their particular country, and in the W&S sector (see Appendix A and B).

Countries in the LAC region have demonstrated efforts to improve cybersecurity protection of their water infrastructure, but existing protections do not fully address the risks. This process requires additional regulation, funding, as well as increased awareness of water facilities by owners and operators.

From the interviews, we identified several tendencies including increased investment in cybersecurity, as management came to recognize that cyber risks affect a variety of operational domains such as commercial, wastewater treatment, water resources and services quality. While some aspects such as the quality of water supply are heavily regulated, the regulation of cybersecurity aspects is often incomplete.

In some LAC countries, most of the operational processes are still being performed manually, with only 15 percent of the systems operated by their water authorities being managed remotely. These trends can be seen in the case of Belize (Belize Crime Observatory, 2020) as described in Figure 8 below.

Figure 8: Priorities in the Belize 2020–2030 Cybersecurity Strategy



National Cybersecurity Strategy

Legal Framework (development of legislation and human resources to detect, investigate and prosecute)

Develop a national capacity for incident reponse and critical information infraestructure protection (establishment of National Incident Reponse capabilities and sectoral Cyber Incident Response Teams [CIRTs])

Workforce Development, Education and awareness in cybersecurity (development of courses relevant to digital economy and society awareness of threats)

Multi-stakeholder Partnership

Source: Belize Ministry of Home Affairs (2020).

The second objective described in the Belize National Strategy published in 2020 refers to minimum security standards for critical information infrastructure systems. The objective is expected to be achieved over the long-term and includes several activities. Among them (Belize Crime Observatory, 2020):

1. Identifying minimum standards for critical information infrastructure.

2. Developing minimum security standards for critical information infrastructure systems.

3. Establishing a working group with the mandate to review threats and recommend standards according to industry.

Cybersecurity in the Water and Sanitation Sector in LAC

Additional issues were also identified based on the interviews:

Lack of official designation of W&S infrastructure as critical. An issue hindering more extensive efforts by official state bodies to improve the cybersecurity of W&S infrastructure is the lack of an official designation of such infrastructure as national CI. This is related mostly to weak national management of CI cyber risks in some countries.

Insufficient internal company cybersecurity teams, as water utilities digitalize. Some LAC water organizations currently use generic industry and vendor "best practices" guides on cybersecurity (for example, firewall policies) and have yet to establish their own. This could be because water systems' digitalization in those countries is relatively new and currently underway, although some of these countries share information and knowledge on cybersecurity solutions for the water industries domestically. In some cases, this may be done in an officially structured manner while in others, it may be done informally, based on personal relationships.

Lack of designated entities for cybersecurity. Another issue preventing countries from having a strong cybersecurity strategy for critical W&S infrastructure is the lack of a designated entity responsible for that issue within the country's water agencies. For example, in one of the LAC countries, a government-owned utility responsible for water supply does not have a dedicated cybersecurity function. Daily cyber operations in this organization are being performed by the IT department, whose employees make up less than 1 percent of the water provider's total number of employees.

New and not yet familiar threats. Some countries in LAC have more advanced mechanisms for managing CI cybersecurity but remain insufficiently prepared for a serious attack against their W&S facilities. Issues affecting preparedness include limited experience dealing with major attacks and limited availability of necessary highly specialized professionals. In one of the most mature countries in LAC in terms of cybersecurity, the largest water and sewage service provider recognizes that the most significant areas of concern facing the sector are the lack of knowledge surrounding the total inventory of IT and OT devices, unsecured industrial infrastructure (i.e., digital assets), and poor training of personnel. From their perspective, this could have an impact on:

Loss of Information

Identity theft

Fraudulent activities

Environmental damage

Reputational damage

Damage to public health

Damage to public infrastructure

In another example, one of the water suppliers who participated in the interviews is regulated by two authorities: one for service quality and the other for technology issues. Although regulation is a major step towards strong cyber defense, the organization only has one employee in the IT department responsible for cybersecurity. Moreover, the organization has no approved cybersecurity procedures, aside from a list of tasks and the need to verify basic controls. Controls, however, are not regulated and are reviewed depending only on their criticality. The organization also lacks a comprehensive annual cybersecurity workplan - it only manages a list of cybersecurity projects, evaluated on an annual basis. It has also never conducted a cybersecurity audit, although a penetration test was done four years prior to the interview. It was revealed the organization used methodologies for securing OT devices in other sectors, and adapted them to the water industry.

Description of the Cybersecurity Status in Five Countries

Country Specific Measures

Several examples of LAC states and their approach to improving their nation's cybersecurity resilience are provided below.

Argentina

In recent years, Argentina has taken multiple measures to implement policies, regulations and reforms in the country's telecommunications, Internet, and technology sectors (IDB and OAS, 2020). In 2008, the country amended the criminal code to include cybercrime. In 2016, the executive branch issued a decree creating the Ministry of Modernization. The decree established the Undersecretariat of Technology and Cybersecurity within the new ministry and placed it in charge of the National Office of Information Technology, the National Directorate of Infrastructure and Operations, and the National Directorate of Critical Infrastructure of Information and Cybersecurity (Privacy International, 2019). In 2017, the Cybersecurity Committee was established under the Cabinet of Ministers and included delegates from the Ministries of Defense and Security. Their mission was to develop a national cybersecurity strategy, which was published in 2019. Decree 50 of 2019 assigned responsibilities regarding CI protection to the Secretary of Public Innovation in the Ministers' Cabinet Office. In early 2023, that same office conducted public consultations to update the National Cybersecurity Strategy.

Argentina was one of the first countries in LAC to have a regulatory framework to protect personal data and is one of the few countries in the Americas that participates in the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Argentine government received an IDB policy-based loan (PBL) in 2019 to support implementation of policies related to CI and practices in the use of ICT in its efforts to strengthen national cybersecurity capabilities and another IDB investment loan in 2023 to protect Critical Information Infrastructure. Argentina has also established a National Program of Critical Infrastructures for Information and Cybersecurity (ICIC) to build a regulatory framework that defines and protects critical and strategic infrastructure belonging to the public and private sectors as well as interjurisdictional organizations. It is also worth noting that Argentina offers a variety of educational opportunities for cyber education in public and private universities as well as civil society, and belongs to cybersecurity working groups with foreign countries (IDB and OAS, 2020).

Brazil

Public and private CI operators in Brazil vary in their maturity in protecting CI. Cybersecurity risk assessments must be performed annually by all federal institutions based on the lessons learned from major cyber incidents. In response to information provided by the Brazilian National Computer Emergency Response Team's (CERT.br) situational awareness tool, all public institutions have clearly defined policies and procedures in place (OAS, 2020). About 54 percent of cyberattacks reported in Brazil originate from within the country (Lewis, 2018).

Chile

Unlike its South American neighbours, the most common cybercrime in Chile is not scam or phishing, but instead malware infection. This trend is the outcome of a technically cyber-educated population that makes use of best practices to keep their devices and data safe. The targets, however, are like those in other Latin American countries: the financial sector, especially banks. To illustrate, Banco de Chile, the country's second-largest bank, suffered a major ransomware attack in May 2018 and lost USD 10 million (Pimenta Klein and Boguslavskiy, 2020). Chile published its National Cybersecurity Policy, including measures to protect CI, in 2017. An updated version is being drafted in 2023.

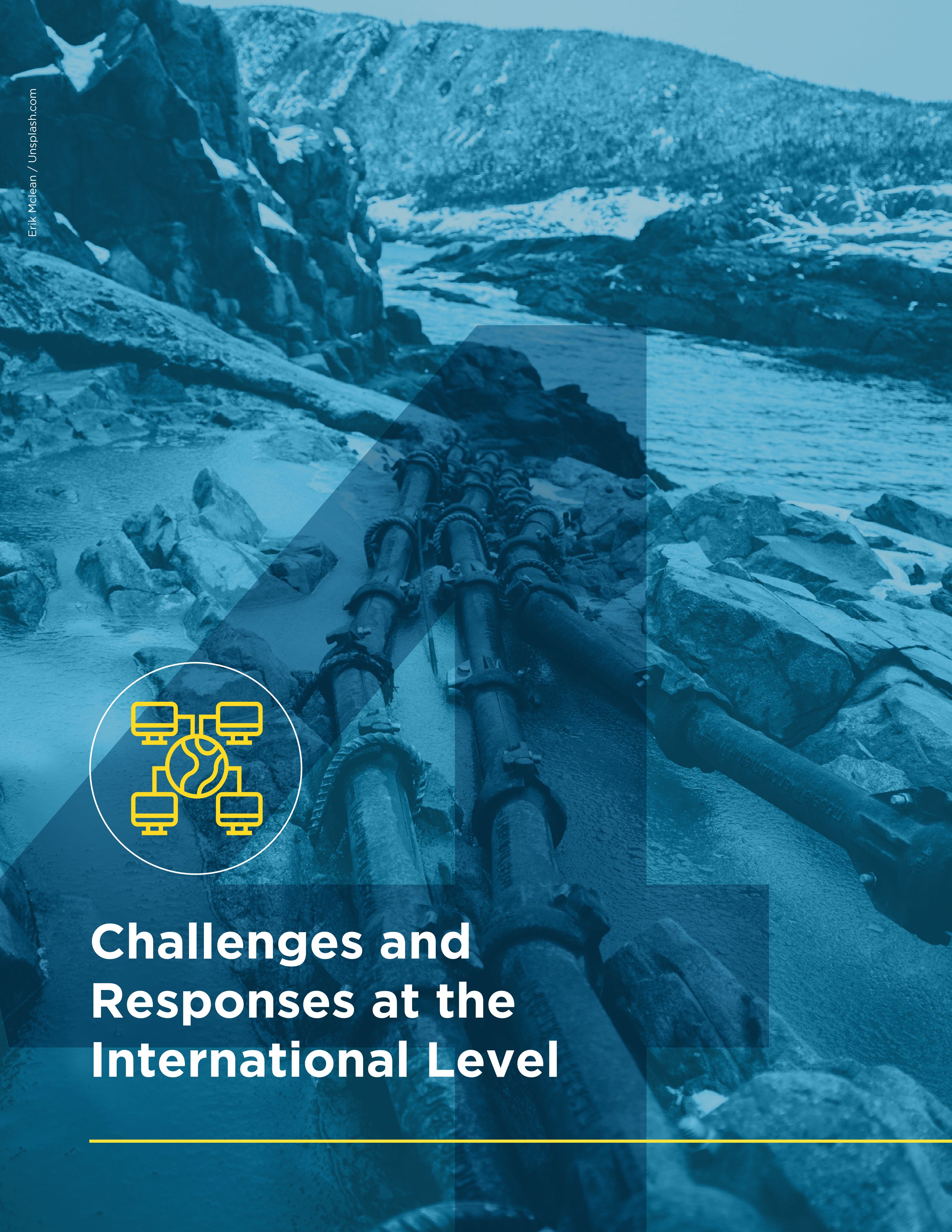
Colombia

Colombia was the first Latin American country to approve a National Cybersecurity Strategy in 2011. Five years later, it implemented an updated strategy known as the National Digital Security Policy. This new version updated the vision of the first policy, this time including risk management (Hernández, 2018). In 2023, the National Development Plan 2023–2026 highlighted the importance of protecting CI and established that a National Digital Security Directorate would coordinate these efforts, as set out in Decree 338 of 2022.

The Dominican Republic

According to a study on the maturity level of national cybersecurity strategies, the Dominican Republic's cybersecurity strategy is considered one of the most mature in LAC, rated by the model as Consolidated. As of 2020, the country's cybersecurity strategy and policy were assessed to have relative weaknesses in crisis management, cyber defense, and communications redundancy, areas in which subsequent advances have now been made. In terms of protection of CI, the Dominican Republic is strongest in organizational aspects, while identification and risk and response management aspects are being improved (IDB and OAS, 2020).

As shown in the preceding examples, the five case studies on national cybersecurity strategy and regulation do not deal specifically with cybersecurity in water infrastructure. The following section will discuss two case studies from Israel and the UK, presenting their national strategy in general terms and, specifically, their regulation for water infrastructure cybersecurity.



Erik Mclean / Unsplash.com

Challenges and Responses at the International Level

Countries around the world are certainly aware of the various potential risks of operating in cyberspace, including the potential damage cyberattacks might inflict on the economy and civilian life, and even considering cases where actors try to advance their geo-strategic goals through online disruptions, posing significant risks to national CI. As this understanding grows, countries are investing more effort toward national cybersecurity and security controls for CPS that underpin mission-critical efforts (Thielemann et al., 2021).

Understanding the Importance of Public-Private Partnerships

Because CI is owned and operated by both public and private actors, and attacks could have wide-ranging effects, the responsibility for protecting it is in the hands of both private and public sector entities. However, the main focus of the two sectors is different. The public sector views infrastructure at a national level and tends to put greater effort into the most strategic assets. Under this approach, governments address CI protection as a collection of systems and services.

In contrast, the private sector prioritizes its profits, standing, and customers, which then leads it to place greater value on service delivery, innovation, cost reduction, and building market share. At the technical level, the private sector puts efforts towards core elements within its direct control or its contractual obligations to deliver services.

These different approaches create opportunities for public-private partnerships at both the strategic and technical levels to bridge these differences and protect CI in a holistic manner. Private organizations should endeavour to understand their role in protecting CI, while governments should appreciate the expert knowledge available in the private sector (OAS, 2018).

International Case Studies

To understand how governments can protect their CI from cyberthreats, with a particular focus on the W&S sector, we present two case studies involving Israel and the United Kingdom. The two models depicted here illustrate national-level regulations established to address cybersecurity risks.

Case Study 1 • The Israeli Model

The government of Israel has addressed issues involving information security and the protection of computerized infrastructure for nearly three decades. Since 1996, it has approved measures to defend against cyberthreats (Tabansky, 2011). In Israel, there is significant emphasis on regulation and coordination between the public and private sectors. Early on, the country designated the W&S sector as CI and has been active in raising awareness of the associated risks. In addition, government cyber authorities allocate resources at the national level to conduct periodic reviews, exercises, and training, thus promoting the importance of focusing on capabilities to protect water infrastructure. These initiatives encourage relevant private entities to enhance their protection and response measures.

Regulation

The Israeli model for protecting infrastructure against cyberthreats is centralized, where a supervisory body closely reviews infrastructure operators' security activities while issuing direct instructions for measures to be taken as needed. In 2002, the Israeli government sought to define responsibilities for the country's computerized systems, including the establishment of a steering committee that determined which bodies would be defined as critical and hence require cyber protection and guidelines (Benoliel, 2014). In 2010, the government established its national cybersecurity authority, currently known as the Israel National Cyber Directorate (INCD). The INCD works to formulate a comprehensive cyberspace protection policy for Israel by handling oversight and regulation of general government activities related to cyberspace from the civilian and national security standpoints (Benoliel, 2014).

Under its regulatory responsibility, Israel's Ministry of Energy and Water, the government office responsible for energy and water infrastructure, works with private infrastructure facilities to protect critical computer systems. Procedures written by the Ministry guide private infrastructure facilities (e.g., gas, and electricity) in securing the critical digital systems they operate.

The Water and Sewage Authority, founded in 2007, is responsible for operating the water supply system at the national, county, and local levels. The mission of the Water and Sewage Authority is to preserve water sources and maintain supply operations, as well as respond to emergency events, such as those that could harm water infrastructure.

The Water Security Unit operates on behalf of the Water and Sewage Authority on the issue of cybersecurity, and handles operations, management, and control of physical and digital water damage incidents, as well as water crises. The unit is also responsible for improving the capabilities of government ministries, national agencies, and water suppliers (desalination plants, water plants, water supply companies), and is involved in preparing for W&S sector incidents by organizing, providing equipment, drafting procedures, and practicing and maintaining the required operational standards.

Israel’s Water and Sewage Authority defined a scale for the level of cyber protection required for water suppliers. Using this scale, each water supplier determines its own level of sensitivity, which consequently determines required cybersecurity controls, as follows:

Level 1 facility or infrastructure:

A. Water supply facilities or infrastructure whose damage will disrupt the functional continuity of water supply to a population of over 250,000 residents.

B. Desalination plant.

C. Sewage treatment plants whose disruption can cause severe and lasting environmental damage.

Level 2 facility or infrastructure:

A. Water supply facilities or infrastructure whose damage will disrupt the functional continuity of water supply to a population of fewer than 250,000 residents.

B. Facilities where self-production of water from drilling is carried out, and there is chlorination.

Level 3 facility or infrastructure:

A. A facility that has no computerized systems deemed essential for the operation of its water and sewage operations.

The Water Security Unit has the exclusive authority to raise the determined level of criticality for a facility based on a weighting of the range of threats, the potential for damage to functional continuity, available manpower, costs, and more.

Attack and response case study

In April 2020, malicious hackers affiliated with Iranian interests allegedly targeted multiple pumping stations and wastewater treatment facilities in Israel, attempting to manipulate chlorine systems to increase chlorine amounts in the water supplied to Israel’s population (Srivastava, 2020). According to published information, the Iranian attack was carried out through servers in the US and Europe in order to hide its origin and reduce suspicion. It reached common off-the-shelf software controllers, which were utilizing PLC programs to operate water pumps. These PLCs were accessible from the Internet, which is how the attackers were able to access them and control the water pumps.

It was reported that the Israeli government responded quickly, ordering all the country’s water and energy facilities to reset the passwords on all their SCADA systems to prevent further attacks. Thanks to the quick response, no significant damage to water quality materialized (Boubaker, 2021). It was then decided to strengthen the security controls protecting SCADA systems, such as disconnecting these systems from the Internet, in order to ensure the continuous operation of these facilities.

Case Study 2 • The UK Model

Regulation

The UK has a long history of using science and technology for national security purposes, and its government has maintained a long-term strategy and policy to support innovation, technology, and knowledge-intensive industries. The British National Security Strategy (NSS), published in 2015, defined cyberthreats as a top threat category and top-level risk to Britain's interests. One year later, the UK published its National Cyber Strategy for 2016–2021 and later updated it for 2022–2030.

The 2022 strategy includes five main objectives:

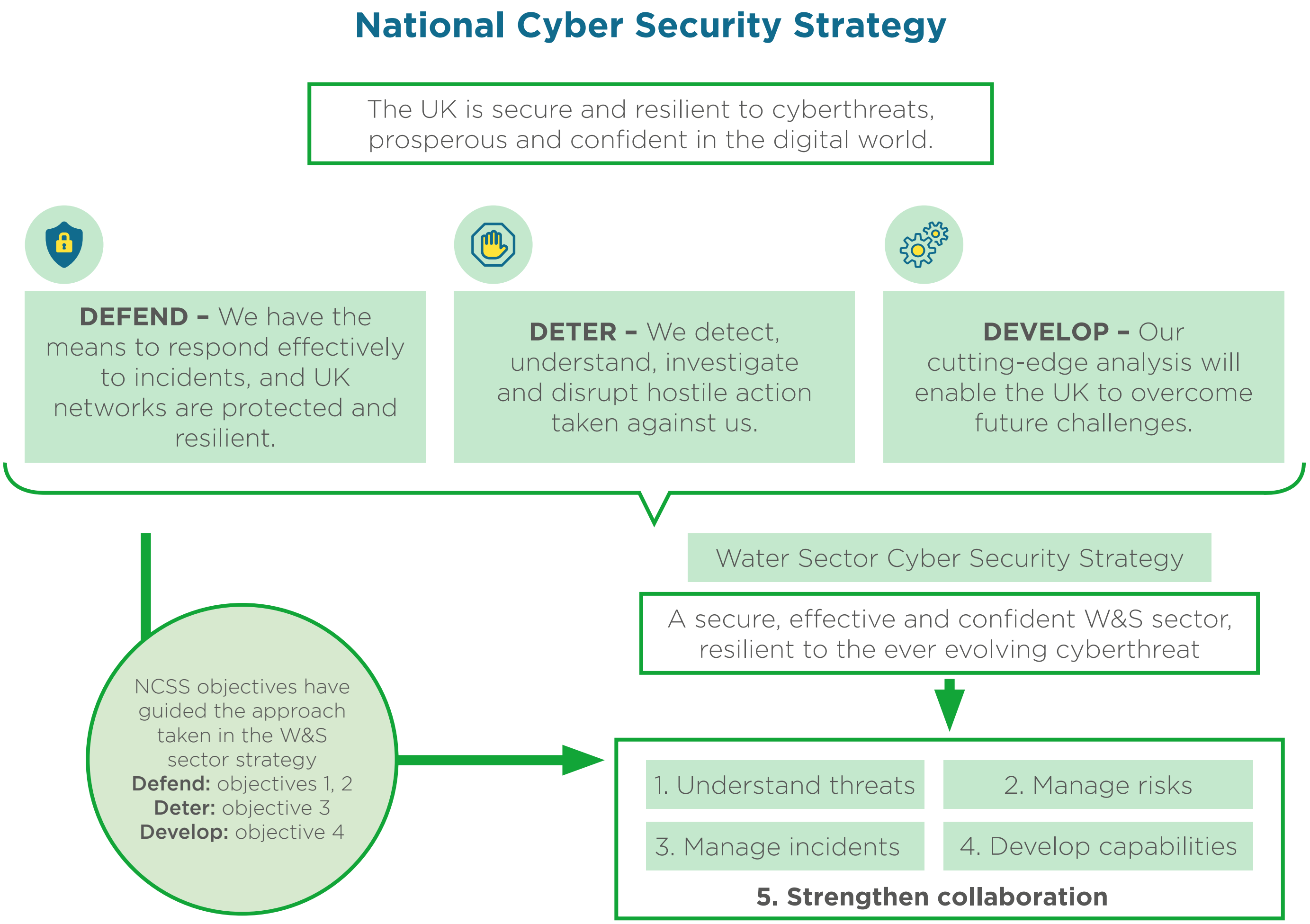
- Manage cybersecurity risks
- Protect against cyberattacks
- Detect cybersecurity events
- Minimize the impact of cybersecurity incidents
- Develop cybersecurity skills, knowledge, and culture

The UK government is investing heavily in carrying out the workplan to achieve the goals set out in the National Cyber Strategy. In 2021 alone, the UK invested £2.6 billion in cybersecurity. This attention given to cybersecurity follows a series of cyberattacks on political institutions, parties, and parliamentary bodies, as well as cyberattacks in which data from British national infrastructure was stolen.

An additional step towards improving cybersecurity is the British cyber institutional reform that established the National Cyber Security Centre (NCSC). The NCSC has been made responsible for governmental operational implementation of all cybersecurity protection in the UK, including issues that were previously under the responsibility of the Centre for the Protection of National Infrastructure.

In 2017, the Department for Environment, Food and Rural Affairs released the Water Sector Cyber Security Strategy for 2017–2021. Its objectives have been guided by the National Cyber Security Strategy (NCSS) outlined in Figure 9 below.

Figure 9: UK National Cyber Security Strategy

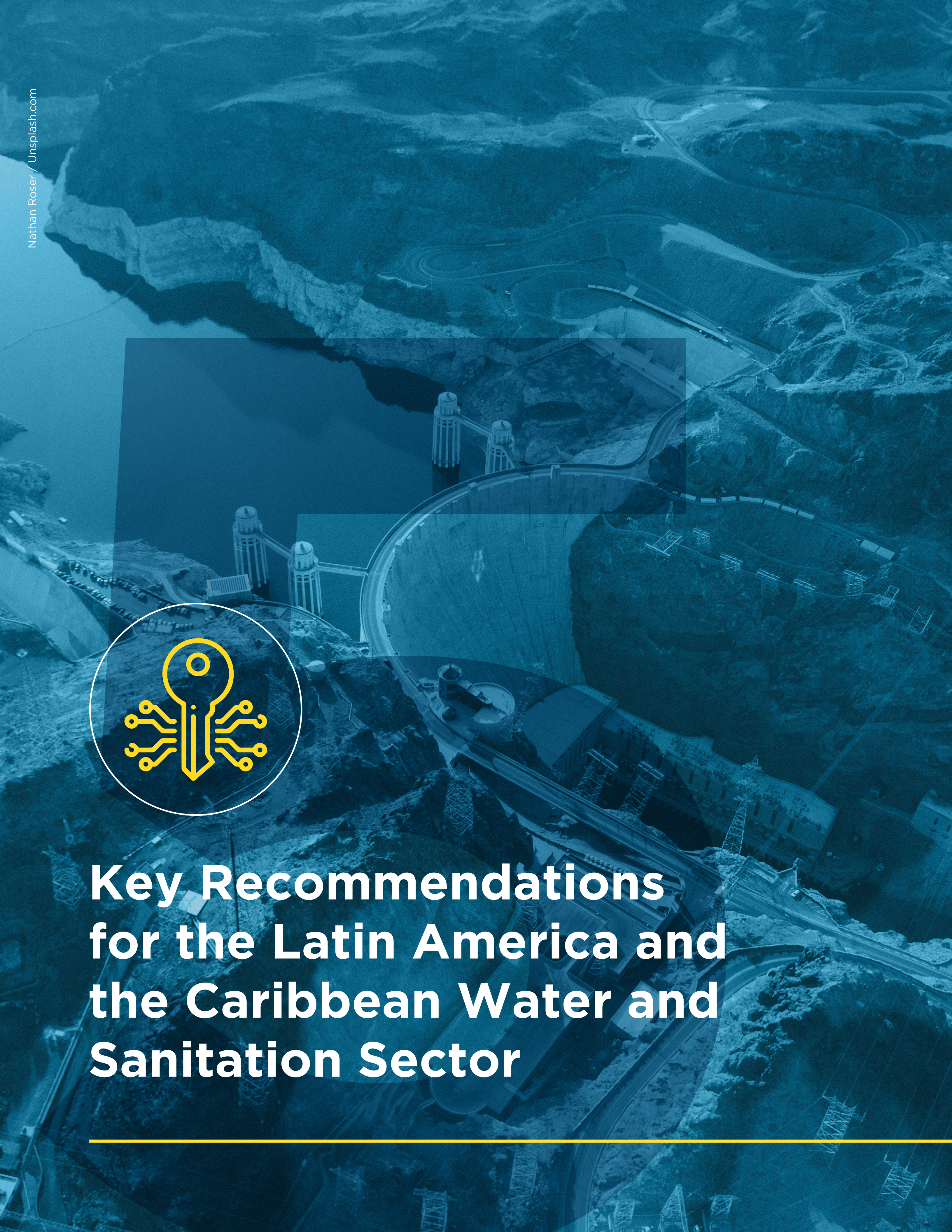

National Cyber Security Strategy
The UK is secure and resilient to cyberthreats, prosperous and confident in the digital world.
DEFEND – We have the means to respond effectively to incidents, and UK networks are protected and resilient.
DETER – We detect, understand, investigate and disrupt hostile action taken against us.
DEVELOP – Our cutting-edge analysis will enable the UK to overcome future challenges.
Water Sector Cyber Security Strategy
A secure, effective and confident W&S sector, resilient to the ever evolving cyberthreat
NCSS objectives have guided the approach taken in the W&S sector strategy
Defend: objectives 1, 2
Deter: objective 3
Develop: objective 4
1. Understand threats
2. Manage risks
3. Manage incidents
4. Develop capabilities
5. Strengthen collaboration

Source: HM Government (2017).

Attack and response case study

Approximately 40 percent of the 777 incidents managed by the NCSC between September 2020 and August 2021 were aimed at government-related entities in the UK. In May 2021, the Irish Health Service Executive suffered a cyberattack. It was announced that the recovery costs from that attack would be USD 600 million (HM Government, 2021).

In such cases, the NCSC plays several roles. First, in partnership with other branches of the government, it identifies threat actors and attributes attacks to them. Second, after detecting a cyber incident, the NCSC analyzes it to assess its characteristics ("NCSC triage incident"). After this assessment, if it is decided that further intervention by the NCSC is needed, support is provided by both a technical team and a legal team. Later, the NCSC coordinates with international entities if needed. Following incidents, insights are shared and new methods for dealing with similar attacks are put forth (HM Government, 2021).



Nathan Roser / Unsplash.com

Key Recommendations for the Latin America and the Caribbean Water and Sanitation Sector

Key Cybersecurity Recommendations

The movement toward industry 4.0 and the resulting convergence of IT and OT has led to the appearance of new cyberthreats for the W&S sector. Several of the water and sanitation organizations interviewed for this study emphasized that they plan further automation and digitalization of their infrastructure in the next 5–10 years. With the W&S sector's increasing digitalization and process automation, establishing appropriate cybersecurity controls is imperative for enhancing resiliency to cyberattacks, and thus supporting the reliability, quality, and confidence of these services.

Below you will find a series of recommendations that follow from the findings of our research and interviews.

Ensure that national, subnational, and local level actors clearly describe their vision and define goals to achieve it

1. Create a **clear and feasible cybersecurity vision,** and detail it in a governmental **CI cybersecurity strategy**. This vision should include clear and capable governance, well-defined and **measurable objectives**, and a road map to accomplish them.

2. **Obtain support and commitment from the government's national leadership** to bolster cybersecurity of the W&S sector and other CI, including the proactive leadership of the national cybersecurity agency, strengthening the human and technical resources available to the sector, and establishing clear governance and operational capabilities to regulate and protect CI.

Create a legal framework in which the water and sanitation sector is recognized as critical infrastructure

1. The first step that needs to be taken is the **formal recognition of the W&S sector as CI**. In most LAC countries, the W&S sector are not officially recognized as CI, often a key factor needed for the sector to receive the required budget and managerial priority with regard to cybersecurity challenges. Without this recognition, the W&S sector will not receive the appropriate attention, and more specifically, insufficient cybersecurity controls will be implemented.

2. In recent years, several countries in the LAC region have modernized their cybersecurity regulatory frameworks, thanks to their increased awareness of the growing importance of this issue, especially for CI systems. Yet efforts at legislation at the national and subnational levels in many of the LAC countries have not yet resulted in coherent implementation of cybersecurity strategies and action plans. Improvements have been made in this respect but activities should be further accelerated. Thus, **the coherent implementation of cybersecurity strategies and action plans, with a focus on CI, must be prioritized**.

3. At the same time, several LAC countries have strengthened their institutional structures both to reduce cyber risks and improve protection and resiliency once those risks materialize, including making investments in processes, people, and technological resources. Such **efforts and interagency coordination are required at the national and international levels** (Saavedra, 2015).

Enzo Tommasi / Unsplash.com

Establish and prioritize public-private partnerships for sharing knowledge

1. Protection of CI must be based on **partnerships that bring together private-private and public-private actors**. To better manage risk, governments, CI owners and operators, and ICT vendors must collaborate across sectors and borders (OAS, 2018). Effective CI security and resilience strategies require public-private partnerships, which in turn make timely, **trusted information sharing among stakeholders essential to the protection of CI** (CISA, 2022).

2. Information sharing also enhances the potential for collective responses to cyberthreats. Organizations are better prepared to thwart attackers and attack methods when **information about cybercriminals and their methods is shared**. Governments would be wise to consider putting in place frameworks and incentives to encourage CI organizations to participate in this activity (OAS, 2018).

3. Public-private partnerships are extremely important in the W&S sector, as it is a sector best described as "conservative" in that it has many professionals employed in the water field, but few cyber experts who can deal with cybersecurity aspects affecting the field. Thus, **creating partnerships between the cyber knowledge found in the private sector and the knowledge found in the W&S sector can expose the W&S sector to industry best practices and cybersecurity know-how**.

4. Public-private partnerships can be effective beyond the simple sharing of actionable threat information. Governments can bring different stakeholders together to improve the security of their critical services by **forming working groups or advisory committees**. Their focus areas could include establishing effective coordinating structures and information-sharing processes and protocols for identifying and exchanging ideas, approaches, and best practices for improving security and international coordination (OAS, 2018).

Helio Dilolwa / Unsplash.com

Understand that public and private organizations and utilities should develop corporate cultures that emphasize cybersecurity

1. **Recognize cybersecurity as a risk**, at the same level as safety, quality of service, environmental protection and other operational priorities.

2. **Increase cybersecurity awareness** by creating a cybersecurity culture with management involvement (e.g., training, tabletop exercises, cyber courses, etc.).

3. **Incorporate security directives** for CI into corporate governance.

4. **Continuously adapt to changes**. The cyberspace domain, including technologies, threats and vulnerabilities, changes rapidly. Recognizing and embracing changes will increase public and private sector recognition and acceptance of national level efforts to create cyber resiliency.

Understand that public and private organizations and utilities should establish and adapt practical steps to be taken within the organizaiton before implementing cybersecurity controls

1. **Map risks and conduct impact assessments** by modeling potential impacts from cyberattacks, including those on human life. These will inform corporate business continuity and data classification schemes.

2. **Map and identify the assets, devices, and systems** involved in your OT/ICS network.

3. **Build an annual and budgeted cybersecurity plan** that will include awareness raising, specific training for relevant teams, cross-company cyber exercises, and the necessary maintenance and upgrading of security solutions.

4. **Prepare and train for incident handling and disaster recovery** by maintaining an updated cyber incident response plan.

5. **Implement cyber security requirements** in all business and technical processes, procurement, supply chains and among contractors.

Formulate cybersecurity solutions for IT and OT convergence of public and private organizations and utilities

1. **Develop a security strategy of relevant cybersecurity standards and procedures for IT and OT systems** (ISO 27001, IEC 64223, etc.) approved by C-level management by deploying a holistic approach where OT, IoT, IIoT, and IT security are managed through a coordinated effort.

2. **Control and minimize OT/ICS network** interfaces with external networks and third parties. Monitor and control needed interfaces on a regular basis.

3. **Nominate dedicated cybersecurity personnel functions** that will oversee IT and OT cybersecurity.

4. **Accelerate security stack convergence by inventorying all OT/ICS IoT security solutions used in your organization**, and evaluate the growing list of stand-alone or multifunctional platform-based options for interoperability with your IT security tools. Segment your OT/ICS network to different zones (layer 0,1, etc.) by deploying proper security controls (firewalls, one-way communication diodes, VLANs, etc.).

Restrict access to the systems in public and private organizations and utilities

1. **Enforce user authentication and role-based access control** to critical process systems.

2. **Implement, monitor, and restrict remote access** when required by employees and third parties. Limit physical access to facilities and systems to authorized personnel.

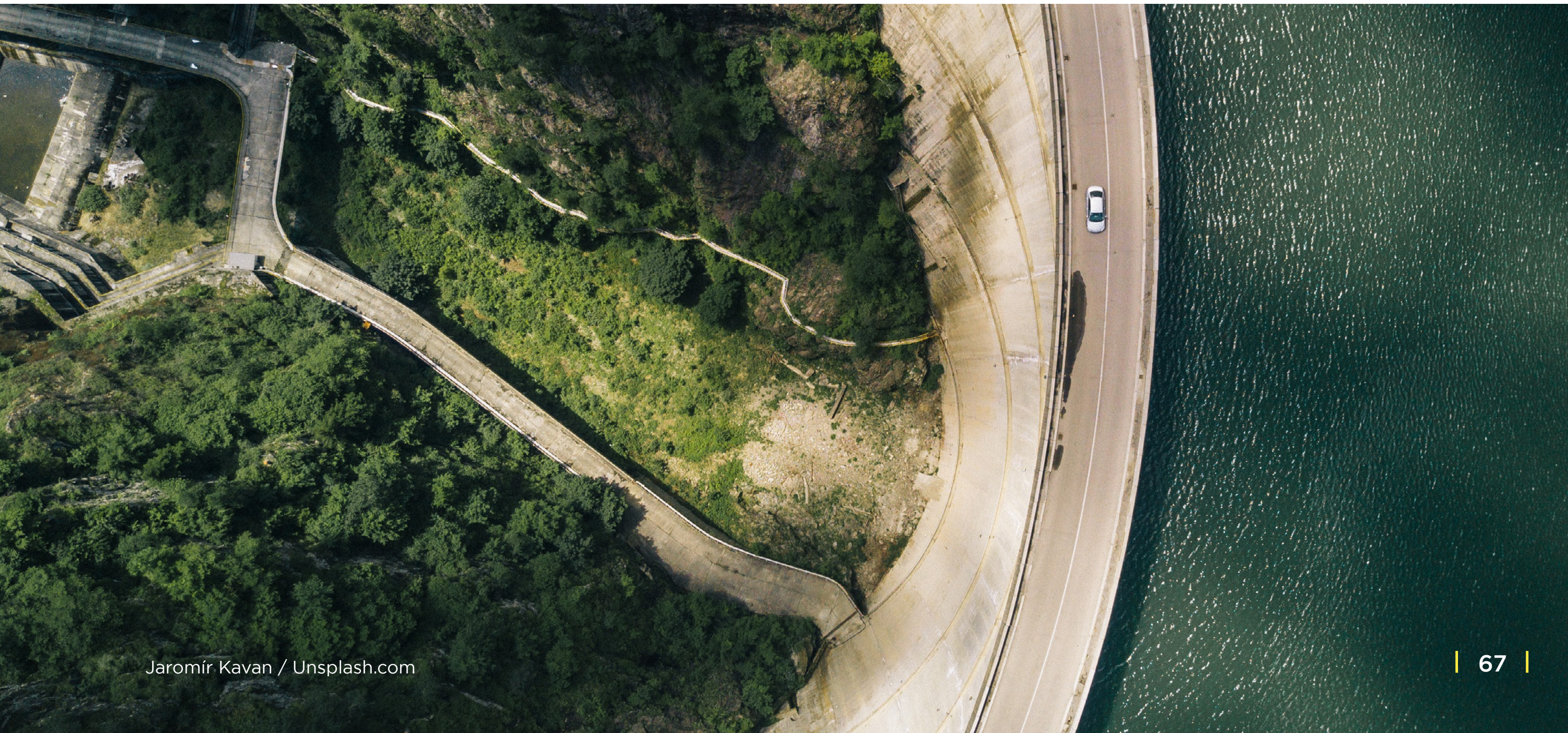
3. **Deploy cyber monitoring systems and threat detection capabilities** (e.g., SIEM, IDS, etc.).

Self-Assessment Questionnaire to Assess the Cybersecurity Scenario Within an Infrastructure

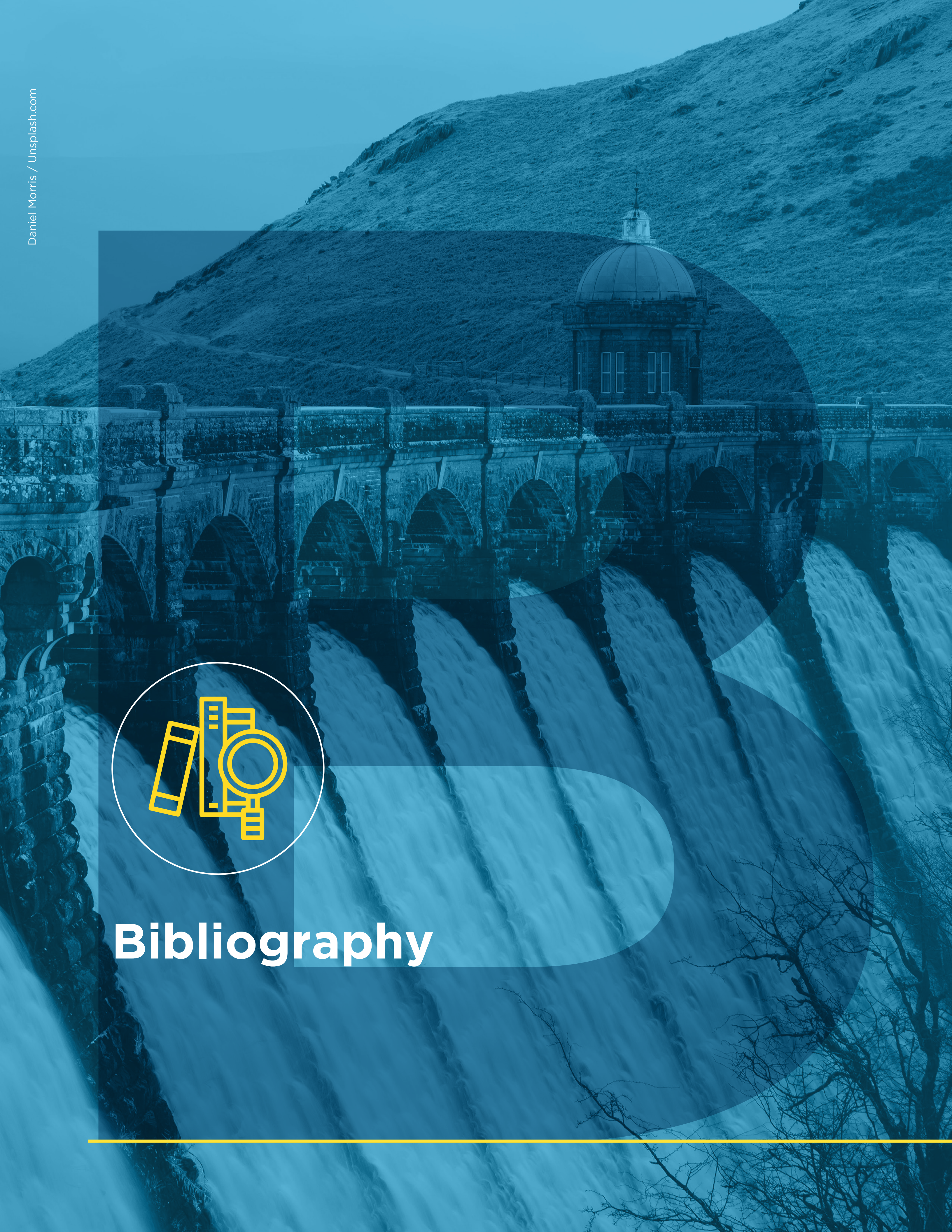
With regard to measuring cybersecurity and making specific recommendations for different entities, the IDB has implemented a tool that will allow water utilities and governments to develop a "road map" for action. It provides an overview and actions to be taken to improve organizations' maturity level, considering the differences between current cybersecurity situations and industry best practices.

The tool, in the form of a **self-assessment questionnaire, allows organizations to evaluate their current cybersecurity infrastructure posture, revealing existing gaps and providing recommendations** that serve as a basis for developing a concrete action plan to address threats.

First, the tool classifies your organization to define three possible risk levels (basic, medium and advanced), according to which it establishes the corresponding information security requirements. Then an **auto-evaluation** is conducted: the questions corresponding to the chosen risk level are presented and the current organizational cybersecurity preparedness is evaluated based on the NIST Cybersecurity Framework (CFS). Finally, the tool calculates a score based on the answers obtained for each NIST-CSF function and category, and provides recommendations to improve the organization's maturity level.



Jaromír Kavan / Unsplash.com



Daniel Morris / Unsplash.com

Bibliography

Bibliography

Ablon, L., and A. Bogart. 2017. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. RAND Corporation. Available at: https://doi.org/10.7249/RR1751.

Ali, H., and J. Choi. 2019. A Review of Underground Pipeline Leakage and Sinkhole Monitoring Methods Based on Wireless Sensor Networking. MDPI Sustainability 11(15), 4007. Available at: https://doi.org/10.3390/su11154007.

Aqualia Group. 2019. The New Reality of Water Management: Industry 4.0. Available at: https://smartwatermagazine.com/news/aqualia/new-reality-water-management-industry-40.

Belize Crime Observatory. 2020. National Cybersecurity Strategy 2020–2023. Belize: The Ministry of Home Affairs & New Growth Initiatives, November 5, 2020. Available at: https://bco.gov.bz/download/national-cybersecurity-strategy-2020-2023/.

Benoliel, D. 2014. Towards a Cyber Security Policy Model: Israel National Cyber Bureau (Incb) Case Study. Global Network of Interdisciplinary Internet & Society Research Centers. Haifa Center of Law and Technology (HCLT). The University of Haifa Faculty of Law, July 2014. Available at: https://law.haifa.ac.il/wp-content/uploads/2021/10/TOWARDS-A-CYBER-SECURITY-POLICY-MODEL-ISRAEL-NATIONAL-CYBER-BUREAU-CASE-STUDY-Daniel-Benoliel-reviewed-version.pdf.

Bigelow, S., and B. Lutkevich. 2021. What Is IT/OT Convergence? Everything You Need to Know. In: Search ITOperations. Available at: https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence.

Boubaker, K.B. 2021. Water Industry: A Look Back at Twenty Years of Cyber Attacks. In Stormshield. Available at: https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water.

Brangetto, P. and M. Kert-Saint Aubyn. 2015. Economic aspects of national cyber security strategies. NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/uploads/2018/10/Economics-of-cybersecurity.pdf.

Canadian Centre for Cyber Security. 2018. An Introduction to the Cyber Threat Environment. Available at: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

Caparros, J. 2021. Top Cyber Threats to Latin America and the Caribbean. Mandiant. Available at: **https://www.mandiant.com/resources/blog/top-cyber-threats-to-latin-america-and-the-caribbean**.

Check Point Software. n.d. Top 8 Types of Cyber Attacks. Available at: **https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/types-of-cyber-attacks/** (accessed May 21, 2022).

Clark, R., S. Panguluri, T. Nelson, and R. Wyman. 2017. Protecting Drinking Water Utilities from Cyberthreats. *Journal of the American Water Works Association* 109. Available at: **https://doi.org/10.5942/jawwa.2017.109.0021**.

Claroty Team82. 2021. Claroty Biannual ICS Risk & Vulnerability Report: 1H 2021. Available at: **https://claroty.com/wp-content/uploads/2021/08/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H_2021.pdf**.

Computer Security Research Center (CSRC). 2022b. Cyber Attack – Glossary. Available at: **https://csrc.nist.gov/glossary/term/Cyber_Attack**.

_______. 2022a. Cyberspace – Glossary. Available at: **https://csrc.nist.gov/glossary/term/cyberspace.**

Cybersecurity & Infrastructure Security Agency (CISA). 2022. Critical Infrastructure Partnerships and Information Sharing. Available at: **https://www.cisa.gov/critical-infrastructure-partnerships-and-information-sharing**.

_______. 2023. Critical Infrastructure Sectors. Available at: **https://www.cisa.gov/critical-infrastructure-sectors**.

Daigger, G. T., N. Voutchkov, U. Lall and W. Sarni. 2019. The Future of Water: A Collection of Essays on 'Disruptive' Technologies That May Transform the Water Sector in the Next 10 Years. Discussion Paper No. IDB-DP-657. Washington, DC: Inter-American Development Bank (IDB). Available at: **https://publications.iadb.org/en/future-water-collection-essays-disruptive-technologies-may-transform-water-sector-next-10-years**.

Deloitte Insights. 2020. Uncovering the Connection Between Digital Maturity and Financial Performance. Available at: **https://www2.deloitte.com/content/dam/insights/us/articles/6561_digital-transformation/DI_Digital-transformation.pdf**.

Deubelli, T. 2019. Towards Resilient and Sustainable Infrastructure: A Case Study of Governance of Critical Infrastructure Resilience in Costa Rica. Washington, DC: Inter-American Development Bank (IDB). Available at: **https://publications.iadb.org/en/towards-resilient-and-sustainable-infrastructure-case-study-governance-critical-infrastructure**.

European Union Agency for Cybersecurity (ENISA). 2023. Critical infrastructure. Available at: **https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services**.

Flashpoint. 2021. From Ransomware to DDoS: Guide to Cyber Threat Actors—How, Why, and Who They Choose to Attack. In: Flashpoint. Available at: **https://www.flashpoint-intel.com/blog/guide-to-cyber-threat-actors/**.

Germano, J. 2019. Cybersecurity Risk & Responsibility in the Water Sector. American Water Works Association. Available at: **https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf**.

Gillette, J., R. Fisher, J. Peerenboom, and R. Whitfield. 2002. Analyzing Water/Wastewater Infrastructure Interdependencies. Infrastructure Assurance Center, Argonne National Laboratory. Available at: **https://publications.anl.gov/anlpubs/2002/03/42598.pdf**.

Global Cyber Security Capacity Centre. 2021. The Cybersecurity Maturity Model for Nations (CMM). Available at: **https://gcscc.ox.ac.uk/the-cmm**.

Guillaume, F. 2022. The Digital Journey of Water and Sanitation Utilities in Latin America and The Caribbean: What is at Stake and How to Begin. Washington, DC: Inter-American Development Bank (IDB). Available at: **https://publications.iadb.org/en/digital-journey-water-and-sanitation-utilities-latin-america-and-caribbean-what-stake-and-how-begin**.

HM Government. 2015. National Security Strategy and Strategic Defense and Security Review 2015: Third Annual Report. Crown copyright, Cabinet Office. Available at: **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819613/NSS_and_SDSR_2015_Third_Annual_Report_-_FINAL__2_.pdf.**

_______. 2017. Water Sector Security Strategy. Department for Environmental Food and Rural Affairs. Available at: **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602379/water-sector-cyber-security-strategy-170322.pdf**.

_______. n.d. Government Cyber Security Strategy: Building a Cyber Resilient Public Sector. Crown copyright, Cabinet Office. Available at: **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf**.

_______. 2021. National Cyber Security Centre (NCSC) Annual Review 2021. Available at: **https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021** (accessed July 9, 2022).

Hernández, J. 2018. National Cybersecurity Strategies in Latin America. Estrategias Nacionales de Ciberseguridad en América Latina. Digital publication for scientific dissemination on strategic studies, war studies, defense policy and security policies. Global Strategy – University of Granada. Available at: **https://global-strategy.org/estrategias-nacionales-de-ciberseguridad-en-america-latina/**.

Inter-American Development Bank (IDB), Organization of American States (OAS). 2016. Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report. Available at: **https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean** (accessed July 8, 2022).

_______. 2020. 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. Available at: **https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean.**

IBM Security. 2021. Cost of a Data Breach Report 2021. Available at: **https://www.ibm.com/downloads/cas/OJDVQGRY**.

International Telecommunication Union (ITU). 2019. ICT Facts and Figures. Available at: **https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf**.

International Water Association (IWA). 2022. Global Trends & Challenges in Water Science, Research and Management. Available at:

https://iwa-network.org/publications/global-trends-and-challenges-in-water-science-research-and-management/.

Kaspersky ICS CERT. 2017a. Península Ibérica y Latinoamérica: estadística de las amenazas para sistemas de automatización industrial, primer semestre de 2017. In: SecureList by Kaspersky. Available at: https://securelist.lat/threat-landscape-for-industrial-automation-systems-in-h1-2017/85531/.

Kaspersky. 2017b. The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within. In: Kaspersky Daily. Available at: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (accessed September 26, 2022).

Lewis, J. 2018. Economic Impact of Cybercrime-No Slowing Down Report. McAfee and the Center for Strategic and International Studies (CSIS). Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

_______. 2020. The Hidden Cost of Cybercrime. McAfee and the Center for Strategic and International Studies (CSIS). Available at: https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf.

Menashri, H., and G. Baram. 2015. Critical Infrastructures and Their Interdependence in a Cyber Attack – The Case of the U.S. Military and Strategic Affairs 7(1). Available at: https://www.inss.org.il/wp-content/uploads/systemfiles/5_Menashri_Baram.pdf.

Mirjana, S., A. Hasanbeigi, N. Neftenov, and Tambourine Innovation Ventures. 2020. Use of 4IR Technologies in Water and Sanitation in Latin America and the Caribbean. Technical Note No. IDB-TN-1910. Washington, DC: Inter-American Development Bank (IDB). Available at: https://publications.iadb.org/en/use-of-4ir-technologies-in-water-and-sanitation-in-latin-america-and-the-caribbean.

Mission of Israel to the UN in Geneva. 2021. Water and Cyber Security – Part II. Available at: https://embassies.gov.il/UnGeneva/NewsAndEvents/Events/Pages/20210413-Water-and-Cyber-Security-Part-II.aspx.

Moore, S. 2021b. Gartner Predicts 30% of Critical Infrastructure Organizations Will Experience a Security Breach by 2025. Available at: https://www.gartner.com/en/newsroom/press-releases/2021-12-2-gartner-predicts-30--of-critical-infrastructure-organi.

_______. 2021a. Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans. Available at: https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we.

Murray, G., M. Johnstone, and C. Valli. 2017. The Convergence of IT and OT in Critical Infrastructure." In: The Proceedings of the 15th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5-6 December 2017, pp. 149-155. Available at: https://doi.org/10.4225/75/5A84F7B595B4E.

Organization of American States (OAS). 2018. Critical Infrastructure Protection in Latin America and the Caribbean 2018. Available at: https://www.oas.org/es/sms/cicte/cipreport.pdf.

_______. 2020. Cybersecurity Capacity Review Brazil 2020. Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford. Available at: https://www.oas.org/en/sms/cicte/docs/ENG-CYBERSECURITY-CAPACITY-REVIEW-BRAZIL.pdf.

Organization for Economic Co-operation and Development (OECD) Water. n.d. Infographic – What Are the Impacts of Water Pollution? Available at: https://www.oecd.org/fr/sites/oecdwater/infographic-impacts-of-water-pollution.htm.

Pimenta Klein, B., and Y. Boguslavskiy. 2020. Latin America Threat Landscape: The Paradox of Interconnectivity. AdvIntel. Available at: https://web.archive.org/web/20230126221027/https://www.advintel.io/post/latin-america-threat-landscape-the-paradox-of-interconnectivity.

Prado, P. 2011. The Impact of the Internet in Six Latin American Countries. Western Hemisphere Security Analysis Center. Available at: https://digitalcommons.fiu.edu/whemsac/6/.

Privacy International. 2019. State of Privacy Argentina. January 23, 2019. Available at: http://privacyinternational.org/state-privacy/57/state-privacy-argentina.

Pursiainen, C., P. Lindblom, P. Francke, and Nordregio. 2007. Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection. Stockholm: Nordregio. Available at: https://www.diva-portal.org/smash/get/diva2:700420/FULLTEXT01.pdf.

Rinaldi, S.M., J. Peerenboom, and T. Kelly. 2001. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, 21(6): 11–25. Doi: 10.1109/37.969131.

Saavedra, B. 2015. Cybersecurity in Latin America and the Caribbean: The State of Readiness for the Defense of Cyberspace. Washington, DC: William J. Perry, Center for Hemispheric Defense Studies. Available at: https://bco.wimp.bz/file_directory/files/cybersecurity/20150730LatinAmericaCaribbeanCybersecurityStateofReadiness.pdf.

Siboni, G., D. Cohen, and A. Rotbart. 2013. The Threat of Terrorist Organizations in Cyberspace. *Military and Strategic Affairs,* 5(3).

Snow, R. 2022. 3 Planning Assumptions for Securing Cyber-Physical Systems of Critical Infrastructure. Gartner Research. Available at: https://www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure.

Srivastava, M. 2020. Israel-Iran Attacks: 'Cyber Winter Is Coming.' Financial Times, 31 May 2020. Available at: https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967.

Stankovic, M., A. Hasanbeigi, and N. Neftenov. 2020. Use of 4RI technologies in water and sanitation in Latin America and the Caribbean. Washington, DC: Inter-American Development Bank (IDB). Available at: https://publications.iadb.org/en/use-of-4ir-technologies-in-water-and-sanitation-in-latin-america-and-the-caribbean.

Stouffer, K., V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn. 2015. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. Available at: https://doi.org/10.6028/NIST.SP.800-82r2.

Tabansky, L. 2011. Critical Infrastructure Protection Against Cyber Threats. Military and Strategic Affairs, 3(2) November 2011. Available at: https://www.inss.org.il/wp-content/uploads/2017/02/FILE1326273687-1.pdf.

Thielemann, K., W. Voster, B. Pace, R. Contu, and R. Hunter. 2021. Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus. Gartner Research, November 17, 2021. Available at: https://www.gartner.com/en/documents/4008351.

US Water Sector Coordinating Council. 2021. Water and Wastewater Systems, Cybersecurity 2021, State of the Sector. Available at: https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf.

Van Raemdonck, N. 2020. Cyber Diplomacy in Latin America. In: EU Cyber Direct, EU Institute for Security Studies. Available at: https://eucyberdirect.eu/research/cyber-diplomacy-in-latin-america.

Water Information Sharing and Analysis Center (WaterISAC). 2021. WaterISAC 2021 Survey. Available at: https://www.waterisac.org/2021survey.

Weiss, J. 2008. Assuring Industrial Control System (ICS) Cyber Security. Applied Control Solutions, LLC, p. 14.

Wesley, C. 2023. What is the CIA Triad? Definition, Explanation and Examples. WhatIs.com. Available at: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.

Williamson, Graham. 2015. OT, ICS, SCADA – What's the Difference? In: KuppingerCole Analysts. Available at: https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference (accessed May 21, 2022).

World Health Organization (WHO). 2019. Water, Sanitation, and Hygiene in Health Care Facilities. Seventy-Second World Health Assembly Agenda item 12.5. Available at: https://apps.who.int/iris/bitstream/handle/10665/329290/A72_R7-en.pdf?sequence=1&isAllowed=y.

Ivan Bandura / Unsplash.com

Dan Meyers / Unsplash.com

Appendices

Appendix A

Interview Questionnaire for Utilities

1. How would you describe your organization?

2. What size is your organization in terms of:

i. number of facilities;

ii. number of employees;

iii. level of production;

iv. annual revenue.

3. Is the organization recognized as a CI? An essential infrastructure? Neither?

4. Who is your regulatory authority?

5. How many people work in the IT department? In cybersecurity?

6. Is there a Cybersecurity Officer position in your organization?

7. What is the approximate budget (in percentage) of your IT department? Your Cyber department?

8. Is cyberthreat recognized as a risk?

9. Are there any cybersecurity regulations, guidelines or requirements coming from the State?

10. Are you aware of any cybersecurity program for the sector at the policy or regulatory level? Please describe.

11. Are there any internal cybersecurity requirements?

12. Is the W&S sector recognized as a CI?

13. Have you suffered from a cyber event/cyberattack? Unexplained maintenance/operational event?

14. How often do you review your cybersecurity controls and procedures?

15. Do you have an annual cybersecurity plan? If so, what does it include (i.e. training, awareness, ethical hacking, device inventory update, etc.)?

16. What is the potential damage of a cyber event (not an attack)? (Financial, Environmental, Public safety or other consequences).

17. When was your last cyber audit? Are there any pending activities?

18. Do you have a cybersecurity training program for employees?

19. Does your utility use secure remote access methods?

20. How would you describe the current and future cyber risks facing the W&S sector in LAC?

21. How would you evaluate the level of preparedness of your state to cyberattacks against CI, and in the W&S sector specifically? How would you evaluate your organization's level of preparedness?

22. To the best of your knowledge, which country in the LAC region has the most robust W&S sector cyber defense management capabilities?

23. Are there cybersecurity tools developed for other sectors (e.g., electrical power grid, oil/gas pipelines) that your utility has adapted for use in the W&S sector?

24. If a threat actor compromised your asset, what realistic worst-case scenarios would result?

25. What interconnections are required for your systems to perform?

26. Have you developed and practiced incident response procedures that combine IT and OT response processes?

Appendix B

Interview Questionnaire for Regulators and Federal Agencies

1. How would you describe your organization?

2. What is the size and resources of the cyber unit overseeing the W&S sector?

3. How would you describe the current and future cyber risks facing the W&S sector in LAC?

4. Is cyberthreat recognized as a risk?

5. How would you evaluate your country's level of preparedness to cyberattacks against CI, and the W&S sector specifically?

6. How would you describe the current and future cyber risks facing the W&S sector in LAC?

7. Are any cybersecurity regulations, guidelines or requirements set by the federal government?

8. Are you aware of any cybersecurity program for the sector at the policy or regulatory level? Please describe.

9. To the best of your knowledge, which country in the LAC region has the most robust W&S sector cyber defense management capabilities?

10. Is the W&S sector officially recognized as a CI?

11. Have you suffered from (or managed) a cyber event/cyberattack?

12. How often do you review your cybersecurity procedures and requirements?

13. Do you have an annual cybersecurity plan? If so, what does it include (i.e., training, awareness, national exercise, etc.)?

14. What is the potential damage of a cyber event in the W&S sector (not necessarily an attack)? (Financial, Environmental, Public safety or other consequences)?

15. Are there cybersecurity tools developed for other sectors (e.g., electrical power grid, oil and gas pipelines) that your organization has adapted for use in the W&S sector?

IDB
IDB | LAB