Cybersicherheit im Wassersektor

Analyse der zukünftigen Entwicklung der Wasser- und Abwasserinfrastruktur

KWB

Verfasser:innen
Dr. Nicolas Caradot
Gruppenleitung
Nicolas.Caradot@kompetenz-wasser.de
+ 49 (0)151 1657 6048

Nikolaus de Macedo Schäfer
Wissenschaftlicher Mitarbeitender
Nikolaus.Schaefer@kompetenz-wasser.de
+49 (0)177 4410526

Elina Henning
Praktikantin

Prüfer:innen
Jean Kolarow
Pascale Rouault

Redaktion
Franziska Sahr

Die Recherchen für diese Studie *w*urden durch eine Reihe von Intervie*w*s ergänzt und vertieft. An dieser Stelle möchte sich das K*W*B bei allen Intervie*w*partner:innen bedanken, insbesondere bei:

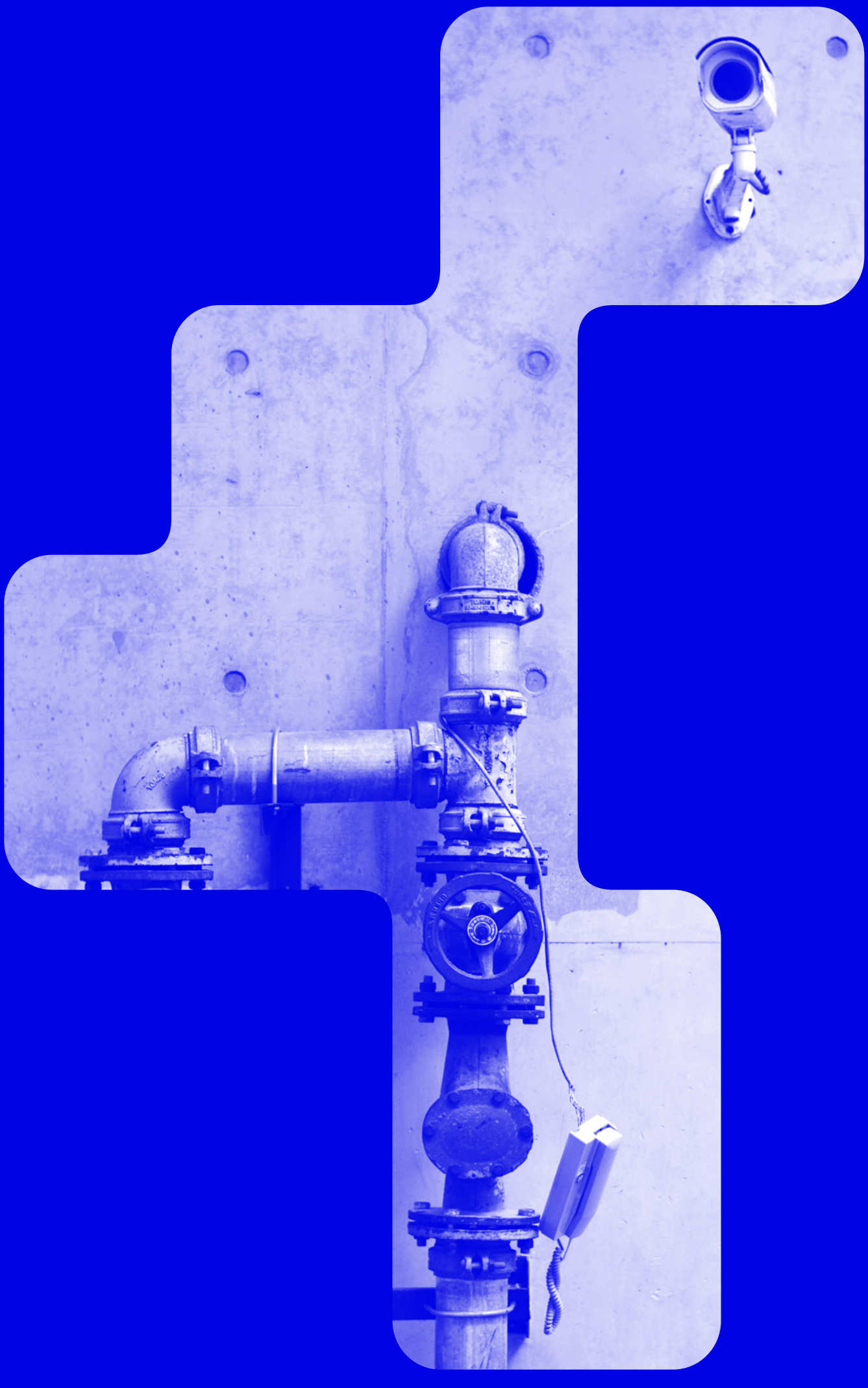
Stadtentwässerungsbetriebe Köln
Berliner Wasserbetriebe
Stadtentwässerung Braunschweig
TU Delft (Riccardo Taormina)
SINTEF (Rita Ugarelli, Martin Jaatun)
Kompetenzzentrum Digitale Wasserwirtschaft
(Ulrike Düwel, Ludger Terhart)
MSF Partners Innovation AG (Rami Efrati)

Inhaltsverzeichnis

Einführung

Dieser Bericht zielt darauf ab, die Transformation des Wassersektors durch die Interpretation der aktuellen und zukünftigen Trends im Zusammenhang mit der Digitalisierung darzustellen. Hauptziel ist es, zukünftige Risiken abzuleiten, die Betreiber ernsthaft in Betracht ziehen sollten, um einen reibungslosen und sicheren digitalen Übergang zu erreichen.

Inhalt



Executive Summary

Im Folgenden nehmen wir Sie mit auf eine kurze Reise durch den bevorstehenden Wandel der Wasserinfrastruktur und zeigen die wichtigsten Trends und Risiken auf, die Betreiber zukünftig berücksichtigen müssen. Ausgehend von der Art der Trends, den damit verbundenen Risiken und dem aktuellen Stand der Cybersicherheitslösungen leiten wir 14 konkrete Forschungs- und Entwicklungsbedarfe ab.

Eine kürzlich von DWA und DVGW durchgeführte Umfrage (KDW 2021) bewertete den aktuellen Stand der Cybersicherheit in der Wasserwirtschaft durch eine Reihe von Interviews mit mehr als 60 deutschen Betreibern. Die wichtigsten Ergebnisse sind aufschlussreich, um den aktuellen Stand der Cybersicherheit im Wassersektor zu verstehen. Nur 12 % der Befragten schätzten ihre eigene Cybersicherheitskompetenz als „gut“ ein, der Rest verteilte sich gleichmäßig auf „mittel“ und „schlecht“. Weniger als ein Fünftel der befragten Wasserbetreiber hatte jemals eine Schwachstellenanalyse seiner industriellen Kontrollsysteme (ICS) durchgeführt. Die Umfrage zeigte ebenfalls, dass die Betreiber in Bezug auf Prävention, Risikobewusstsein und Handlungsbereitschaft eine große Bandbreite an Praktiken anwenden.

Weniger als ein Fünftel der befragten Wasserbetreiber hat bisher eine Schwachstellenanalyse seiner industriellen Kontrollsysteme (ICS) durchgeführt.

Die wachsenden Risiken im Zusammenhang mit der Cybersicherheit stehen in direktem Zusammenhang mit der digitalen Transformation des Wassersektors (GWRC 2021). Während digitale Technologien das Potenzial haben, das Management unserer Wasserinfrastrukturen zu verändern, stellen sie die Betreiber auch vor erhebliche Herausforderungen bei der Aufrechterhaltung der Cybersicherheit (IWA 2019).

Die Digitalisierung verschafft den Betreibern neue Möglichkeiten, die Komplexität miteinander verbundener Infrastrukturen zu bewältigen, und wird heute als unabdingbare Voraussetzung für die Bewältigung zentraler Problematiken – wie die Urbanisierung, der Klimawandel, die alternden Infrastrukturen und die Transformation des Arbeitsmarktes – angesehen. Digitale Technologien sind zwar von grundlegender Bedeutung für die Bewältigung der künftigen Herausforderungen der städtischen Wasserwirtschaft, doch die Einführung vernetzter und integrierter digitaler Lösungen führt zu neuen Problemen der Cybersicherheit. Insbesondere die zunehmende Vernetzung und Automatisierung des Wassersektors schafft neue Schwachstellen für böswillige Cyberaktivitäten.

In diesem Kontext zielt dieser Bericht darauf ab, die Transformation des Wassersektors durch die Interpretation der aktuellen und zukünftigen Trends im Zusammenhang mit der Digitalisierung darzustellen. Hauptziel ist es, eine Reihe von zukünftigen Risiken abzuleiten, die Betreiber ernsthaft in Betracht ziehen sollten, um einen reibungslosen und sicheren digitalen Übergang zu erreichen.

Die Reise der Digitalisierung beginnt mit Daten, die heute als das neue Gold der modernen Betreiber gelten. IoT-Lösungen und eine neue Generation von Sensoren werden zunehmend eingesetzt, um die Überwachung, das Verständnis und die Kontrolle von Infrastrukturen und Ressourcen zu unterstützen **(Trend 1: IoT und intelligente Sensoren)**. Die zunehmende Verbreitung von IoT-Geräten, die „Big Data“ mit hoher Auflösung und Frequenz erzeugen, stellt die Betreiber vor die Herausforderung, diese Daten in ein wertvolles Produkt umzuwandeln. Die zunehmende Vernetzung von IoT-Sensoren mit dem Internet wird neue Angriffsflächen und Schwachstellen schaffen. Die Datenübertragung und IoT-Plattformen werden immer anfälliger für böswillige Angriffe und die Betreiber müssen neue Lösungen finden, um diese neuen heterogenen Komponenten sicher in die bestehende Infrastruktur zu integrieren. Eine stärkere Zusammenarbeit mit Sicherheitsexpert:innen wird für die erfolgreiche Umsetzung des Wasser 4.0 zwingend notwendig sein. Zudem stellt die Vernetzung der informationellen und operationellen Ebenen auch neue Qualifikationsanforderungen dar, für die entsprechende Bildungsmaßnahmen erforderlich sind.

In den letzten zehn Jahren ist das generierte Datenvolumen exponentiell gestiegen. Parallel dazu hat der wachsende Zugang zu Rechenleistung die Möglichkeit geschaffen, Daten zu analysieren, das Verhalten komplexer Systeme zu verstehen und die Funktionsweise natürlicher und städtischer Systeme zu simulieren **(Trend 2: KI für die Wasserwirtschaft)**. Das maschinelle Lernen wird den Wert von Daten extrahieren und Betreibern neue Planungskapazitäten bieten, z. B. für die Vorhersage von Wasserbedarf und -verbrauch, die Umsetzung von vorausschauenden Wartungsstrategien oder die Entwicklung digitaler Zwillinge unserer Infrastrukturen (Mehmood et al. 2020). Es wird erwartet, dass KI auch eine Schlüsselrolle für die Cybersicherheit im Wassersektor spielen wird. Die KI-Modellierung wird in zunehmendem Maße zur Lösung verschiedener Cybersicherheitsprobleme und -aufgaben eingesetzt werden, z. B. zur automatischen Identifizierung bösartiger Aktivitäten, zur Erkennung von Phishing, zur Erkennung von Anomalien oder Eindringlingen usw. Der zunehmende Einsatz von KI durch Wasserbetreiber wird auch neue Bedenken

hinsichtlich der Zuverlässigkeit von Vorhersagen und des Schutzes von Algorithmen vor gezielten Cyberangriffen aufwerfen, die darauf abzielen, die Kontrolle über den Algorithmus zu erlangen und sein Verhalten zu ändern. So könnten Angreifer beispielsweise absichtlich eine minimale Menge fehlerhafter Daten in den Steuerungsalgorithmus einer Anlage einspeisen, um deren Verhalten zu ändern und die Dosierung von Chemikalien für die Trinkwasseraufbereitung oder andere kritische Vorgänge zu beeinflussen.

Die zunehmende Verbreitung von IoT- und Modellierungstools geht mit dem Aufkommen von Cloud-Lösungen und Software-as-a-Service einher, die sich voraussichtlich durchsetzen werden **(Trend 3: Cloud-Migration)**. Das Tempo der Einführung von Cloud-Lösungen beschleunigt sich eindeutig, während das Spektrum der Anwendungen, die in die Cloud verlagert werden, zunimmt und langsam auch sensible Bereiche wie industrielle Kontrollsysteme und Betriebstechnologien (OT) erreicht. Bis heute haben die meisten Betreiber ihre IT- und OT-Netzwerke logisch oder sogar physisch getrennt und sich auf autonome Zonen verlassen, die auch bei einem Ausfall anderer Zonen unabhängig weiterarbeiten können. Mit dem Aufkommen des IoT beginnen Betreiber, Daten und Analysen in das ICS zu integrieren, um die Überwachung, aber auch die Kontrollkapazität des Betriebs zu verbessern. Es wird erwartet, dass die Cloud-Migration von ICS- und Supervisory Control and Data Acquisition Architecture (SCADA)-Systemen eine höhere Effizienz und Zuverlässigkeit bietet, die Systeme aber auch neuen Quellen für neue Bedrohungen und Schwachstellen aussetzt (Taormina et al. 2017). In Deutschland nehmen die politischen Entscheidungsträger diese Bedrohung sehr ernst: Eine kürzlich erfolgte Überarbeitung des Industriestandards B3S WA („Branchenspezifischer Sicherheitsstandard Wasser/Abwasser“) beinhaltet wichtige Änderungen wie die Verpflichtung für Betreiber, innerhalb der nächsten eineinhalb Jahre Angriffserkennungssysteme sowie neue spezifische Anforderungen in Bezug auf Datenaustausch, Virtualisierung, IoT-Geräte, Intrusion Detection und Cloud Computing zu implementieren (Marquardt 2021).

Die neue technologische Landschaft, die sich durch das Zusammentreffen der drei oben genannten Trends ergibt, bietet den Betreibern neue Instrumente für die Gestaltung der Entwicklung der städtischen Wasserinfrastruktur **(Trend 4: Transformation der Infrastruktur)**. Die Nachteile zentralisierter Infrastrukturen stellen ihre Wirksamkeit im Hinblick auf die Nachhaltigkeit in Frage und die Hauptnachteile traditioneller Wassernetze werden immer deutlicher. Die aktuellen technologischen Fortschritte begünstigen die Entstehung neuer hybrider und dezentraler Systeme wie nachhaltige Regenwasserbewirtschaftung, Wasserwiederverwendung, Quellentrennung und dezentrale Aufbereitung. Es zeichnet sich bereits ab, dass konventionelle Netze wahrscheinlich nicht als Folge einer disruptiven Innovation verschwinden werden.

Der Wassersektor wird oft als konservativ und resistent gegenüber Veränderungen beschrieben. Diese Risikoscheu hängt eindeutig mit dem Investitionscharakter der Infrastruktur, der Pfadabhängigkeit früherer Entscheidungen und historischer Entwicklungen und natürlich mit dem Ausmaß möglicher Fehlschläge zusammen. Anders ausgedrückt: Für Betreiber lohnt es sich im Allgemeinen weniger, die für Innovationen erforderlichen Risiken einzugehen, als dass sie für Misserfolge bestraft werden (Kiparsky 2013). Neben den massiven Hindernissen für die Einführung – die natürlich nicht nur technischer Natur sind, bspw. bilden fehlende Kompetenzen und Fachkräfte große Hürden – wird die Umgestaltung der Infrastruktur die derzeitige Architektur unserer Systeme verändern und könnte die Quelle für neue Schwachstellen und Sicherheitsprobleme sein. Ein gutes Beispiel sind neue Ansätze für die Regenwasserbewirtschaftung, bei denen es um die Integration heterogener blau-grüner Infrastrukturen in die herkömmlichen städtischen Entwässerungssysteme geht. Die Notwendigkeit der Kontrolle grüner Infrastrukturen in Verbindung mit ihrer Heterogenität in Bezug auf Art, Umfang und Funktion wird zu neuen Cyberrisiken führen. Neue Governance-Formate, wie die Verlagerung der Verantwortung für die Installation, den Betrieb und die Instandhaltung grüner Infrastrukturen von öffentlichen Betreibern auf die Grundstückseigentümer:innen, werden auch zu Bedenken hinsichtlich der Rolle einzelner Akteure beim Schutz der Daseinsvorsorge führen.

Schließlich prägt die Vision der Smart City die Zukunft der Wasserwirtschaft, da öffentliche Infrastrukturen, Dienstleistungen und Verwaltungen (z. B. Wasser, Abwasser, Verkehr, Stadtplanung, Energie usw.) durch den Einsatz digitaler Lösungen und Plattformen zunehmend miteinander verbunden werden **(Trends 5: Smart City und die neue Rolle des Wassers)**. Die Stadt der Zukunft durchbricht die traditionellen vertikalen Silos der Verwaltungen und nutzt Daten aus verschiedenen Bereichen, um datengestützte Entscheidungen zu treffen und das

Engagement der Bürger:innen zu fördern. Der zunehmende Informationsaustausch in der intelligenten Stadt bringt zwangsläufig erhöhte Risiken und Bedenken hinsichtlich der Datensicherheit und des Datenschutzes mit sich. Insbesondere die unglaubliche Größe, Komplexität und Heterogenität der neuen städtischen Datenplattformen wird die öffentlichen Akteure vor die Herausforderung stellen, umfassende Cybersicherheitsstrategien zu entwickeln und Kaskadeneffekte zu bewältigen.

Dieser Bericht nimmt Sie mit auf eine kurze Reise durch den bevorstehenden tiefgreifenden Wandel und zeigt einige der wichtigsten Trends und Risiken auf, die die Betreiber der Zukunft berücksichtigen müssen. Da das „Wasser 4.0 bereits da ist“ (IWA 2019), wirken sich einige dieser Veränderungen bereits auf Betreiber aus und lösen digitale Innovationen und F&E-Programme aus. Ausgehend von der Art der Trends, den damit verbundenen Risiken und dem aktuellen Stand der Cybersicherheitslösungen leiten wir 14 konkrete Forschungs- und Entwicklungsbedarfe ab.

Wir hoffen, dass diese Perspektiven den Betreibern und dem gesamten Wassersektor auf ihrem Weg zu widerstandsfähigeren und cyber-sicheren Wasserinfrastrukturen helfen können.

Forschungs- und Entwicklungsbedarf

- **Verbesserung der Sicherheit von IoT-Komponenten**
- **Aufbau von KI-basierten fortschrittlichen Analysen für Cybersicherheitsprobleme**
- **Erfassung des realen Verhaltens von Analyst:innen bei der Entwicklung von KI-Algorithmen**
- **Reduzierung der Einschränkungen von KI und Erhöhung der Robustheit von Vorhersagen**
- **Verbesserung des Verständnisses für neue Sicherheitsprobleme im Zusammenhang mit der Konvergenz von IT- und OT-Systemen**
- **Unterstützung der Verlagerung von ICS von eigenständigen Systemen zu Cloud-basierten Umgebungen**
- **Experimentieren mit Testbeds und Simulationsumgebungen**
- **Entwicklung sicherer Lösungen, die die Dezentralisierung der Infrastruktur begleiten**
- **Erstellung einer strukturellen Ontologie für Smart Cities**
- **Verbesserung der Sicherheit von städtischen Datenplattformen**
- **Vermeidung von Kaskadeneffekten und Entwicklung von Abhilfestrategien**
- **Entwicklung flexibler Cybersicherheitsansätze für kleine und mittelgroße Betreiber**
- **Verstärkung der lokalen, regionalen und internationalen Zusammenarbeit im Wassersektor**
- **Entwicklung neuer und verbesserter Ausbildungs- und Schulungsprogramme und Erhöhung der Attraktivität des Sektors für IT- und OT-Expert:innen**

Einleitung

Die anhaltenden Herausforderungen der Urbanisierung, des Klimawandels und der alternden Infrastruktur sind Haupttreiber der digitalen Transformation der Wassersysteme. Neben Potenzialen birgt die Digitalisierung allerdings auch erhebliche Risiken. Die Anzahl der Cyberangriffe auf kritische Infrastrukturen wächst rasant und Betreiber sehen sich vor neuartige Herausforderungen gestellt.

Cybersicherheit im Wassersektor: Risiken im digitalen Zeitalter

Die Wasser- und Abwasserinfrastruktur gilt als kritische Infrastruktur, da sie für die Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen unerlässlich ist (European Commission 2021). Die Bereitstellung von sauberem Trinkwasser ist für die Gesundheit der Gesellschaft ebenso notwendig wie die effiziente Beseitigung und Entsorgung menschlicher Abfälle über die Abwassersysteme (Birkett 2017). Schäden an kritischen Infrastrukturen, ausgelöst durch Naturkatastrophen, Terrorismus, kriminelle Handlungen oder etwa mutwillige Zerstörung, können schwerwiegende Auswirkungen auf die Sicherheit und das Wohlergehen der Bürger:innen haben, weshalb der Schutz der Infrastrukturen von höchster Relevanz und politischer Priorität ist (BBK o. J.).

Cyberangriffe sind für alle kritischen Infrastrukturen fast alltäglich und werden von der deutschen Regierung als große Bedrohung angesehen. Aufgrund der Covid-19-Pandemie hat sich die öffentliche Aufmerksamkeit allerdings auf Vorfälle im Gesundheitswesen konzentriert (BSI 2021). Über die Anzahl der jährlichen Cybersicherheitsvorfälle im Wassersektor gibt es hingegen in Deutschland und weltweit nur sehr wenige Informationen. Im Jahr 2015 reagierte das US-Ministerium für Heimatschutz auf 25 Cybersicherheitsvorfälle im Wassersektor und auf 46 Vorfälle im Energiesektor (Clark et al. 2016). In einem weiteren Bericht wurde festgestellt, dass 54 % der 500 befragten US-Betreiber für kritische Infrastrukturen über Angriffe berichteten, die das Ziel hatten, die Systeme unter Kontrolle zu bringen, während es 40 % der berichteten Angriffe darauf abgesehen hatten, die Systeme abzuschalten (Trend Micro 2015). Eine kürzlich veröffentlichte Umfrage unter 179 Betreibern in den USA, Deutschland, dem Vereinigten Königreich und Australien ist noch alarmierender: Darin wird hervorgehoben, dass 87 % in den vorangegangenen 36 Monaten mindestens eine Verletzung der OT-Sicherheit beobachtet hatten (Skybox Security 2021). In Deutschland wurde mit dem IT-Sicherheitsgesetz eine Meldepflicht von Cyber-Vorfällen für Betreiber kritischer Infrastrukturen eingeführt (§ 8b Abs. 4 BSI-Gesetz). Im Jahr 2020 gingen beim BSI 419 entsprechende Meldungen ein, davon 73 aus dem Energiesektor und nur sieben aus dem Wassersektor (BSI 2020). Diese Zahlen sind nicht vollständig repräsentativ für die Branche und wahrscheinlich nur die Spitze des Eisbergs, da viele Cybersicherheitsvorfälle entweder unentdeckt bleiben oder einfach nicht gemeldet werden, um den Ruf des Betreibers, das Vertrauen der Kund:innen und folglich auch die Einnahmen nicht zu schädigen (Hassanzadeh 2020).

Die öffentliche Wahrnehmung von Cyberrisiken wird oft durch isolierte und spektakuläre Ereignisse geprägt, die das Ausmaß der Bedrohung unterstreichen. So wurde beispielsweise 2019 eine kleine Stadt mit 35 000 Einwohner:innen nördlich von West Palm Beach in den USA durch einen Ransomware-Angriff lahm gelegt, nachdem ein Mitarbeiter der Polizeibehörde eine infizierte E-Mail geöffnet hatte. Der Angriff griff auf den Wasserversorger über und beeinträchtigte die Computersysteme, die die Pumpstationen, die Wasserqualitätsprüfung sowie die Zahlungsvorgänge steuern. Die Kommunalverwaltung musste mehr als 600 000 US-Dollar Lösegeld zahlen, um den Angriff rückgängig zu machen und Zugang zu den Daten zu erhalten (Mazzei 2019). In jüngerer Zeit gelang es Hackern, aus der Ferne auf die Wasseraufbereitungsanlage der Stadt Oldsmar in Florida zuzugreifen und den Laugengehalt des Trinkwassers kurzzeitig zu ändern. Der Natriumhydroxid-Gehalt wurde von 100 mg/l auf 11 100 mg/l erhöht, eine Menge, an der die Bewohner:innen schwer hätten erkranken können, wenn sie das verseuchte Wasser über einen längeren Zeitraum getrunken hätten. Dieser Überfall wurde rein zufällig gestoppt, als ein Mitarbeiter bemerkte, dass jemand seinen Computer kontrollierte (Robbles und Perlroth 2021).

Für einen Überblick über Cybervorfälle im Wassersektor

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. Journal of Environmental Engineering, 146 (5): 1-13.

Das Potenzial der Digitalisierung und die Treiber der digitalen Transformation

Die zunehmenden Risiken im Zusammenhang mit der Cybersicherheit sind natürlich mit der digitalen Transformation des Wassersektors verbunden (GWRC 2021). Die International Water Association schätzt, dass das „Wasser 4.0 bereits da ist“ und betont, dass das Wasser 4.0 von Betreibern nicht mehr als „Option“, sondern als „Notwendigkeit“ angesehen wird.

Digitale Technologien bieten ein enormes Potenzial, die Verwaltung unserer Wasserinfrastrukturen zu verändern, bringen aber auch neue Herausforderungen für die Aufrechterhaltung der Cybersicherheit mit sich (Sarni et al. 2019). Leistungsstarke digitale Technologien wie mobile Geräte, Sensornetzwerke, Cloud Computing, maschinelles Lernen (ML) und Modellierungswerkzeuge haben das Potenzial, das Management von Wasserinfrastrukturen und die Qualität der für die Bürgerinnen und Bürger erbrachten Dienstleistungen drastisch zu verbessern (ICT4Water 2018). Die Liste der Versprechen der Digitalisierung ist lang und verlockend: Digitale Lösungen können die Kontrolle und Effizienz von Wassersystemen verbessern, die Überwachung der Wasserqualität erleichtern, das Management und die Entscheidungsfindung unterstützen, die Resilienz und Sicherheit der Infrastruktur erhöhen, die Interaktion zwischen Betreiber, Behörden und Kunden vereinfachen.

Kurz gesagt, die Digitalisierung gibt den Betreibern neue Möglichkeiten, die Komplexität der vernetzten Infrastrukturen zu bewältigen und die Entscheidungsfindung in einer sich ständig verändernden Landschaft zu unterstützen (Makropoulos und Savić 2019). Die Betreiber nutzen die Digitalisierung jedoch nicht nur, um ihre Servicequalität und ihre Einnahmen zu steigern oder um einem globalen Trend zu folgen. Die anhaltenden Herausforderungen der Urbanisierung, des Klimawandels und der alternden Infrastruktur sind Haupttreiber der digitalen Transformation der Wassersysteme (GWRC 2021).

Insbesondere die Auswirkungen der alternden Wasserinfrastruktur werden immer deutlicher. Bereits vor zehn Jahren schätzte die American Water Works Association, dass eine neue Ära anbricht: die Ära der Erneuerung, in der das Land die von den vorangegangenen Generationen gebauten Wasser- und Kanalisationsnetze massiv sanieren muss (AWWA 2012). Die aktuelle Situation ist nicht viel besser. Zwischen 2012 und 2018 ist die Zahl der Wasserleitungsbrüche in den USA um fast 30 % gestiegen (Folkman et al. 2018) und die jährliche Investitionslücke bei der Trinkwasserversorgung und Abwasserentsorgung wird bis 2029 auf 434 Milliarden US-Dollar geschätzt (ASCE 2020). In dem Bestreben, intelligentere Investitionen zu tätigen, beschleunigt die Branche die Einführung digitaler Lösungen zur Verbesserung und Optimierung ihrer strategischen und betrieblichen Planungsfähigkeiten (Chastain-Howley 2018).

Neben der allgemeinen Veralterung der Anlagen haben die Betreiber auch mit der Herausforderung zu kämpfen, dass Arbeitskräfte in den Ruhestand gehen (120water 2021), da die meisten erfahrenen Mitarbeiter:innen das Rentenalter erreichen. Im Vereinigten Königreich rechnen die Wasserbetreiber mit einem Fachkräftemangel von 27 000 Personen bis zum Ende des Jahrzehnts und beginnen mit der Entwicklung neuer Strategien, um neue Talente anzuziehen und zu halten (Aquatech 2021). In den USA müssen Betreiber in den nächsten zehn Jahren möglicherweise 30 % bis 50 % ihrer Belegschaft erneuern (Dickerson et al. 2018). Der akuteste Fachkräftemangel wird in Ingenieur- und Technikerberufen, aber auch in branchenübergreifenden Disziplinen wie Datenwissenschaften, künstlicher Intelligenz und besonders in der Cybersicherheit zu verzeichnen sein. Betreiber rechnen mit Schwierigkeiten bei der Sicherstellung ausreichender Fachkenntnisse im Bereich der Betriebstechnologien, um dem wachsenden Bedarf an Überwachung und Steuerung unserer Anlagen und Netze gerecht zu werden (BSI 2015). Der Sektor unternimmt bereits beträchtliche Anstrengungen, um seine Attraktivität zu steigern. In einem gemeinsamen Statement von Fachverbänden der Wasserwirtschaft und der Länderarbeitsgemeinschaft Wasser zur Fachkräftesicherung und -qualifizierung für die Wasserwirtschaft werden neben den Risiken, die dieser Fachkräftemangel für die Zivilgesellschaft mit sich bringt, auch erste Handlungsempfehlungen formuliert. Dazu gehören die Stärkung des Wasserbewusstseins in der Bevölkerung und in der Politik oder eine attraktive Gestaltung des fachlichen Qualifizierungsangebotes (LAWA et al. 2021).

Als weiterer Schlüssel zur Erfassung und Weitergabe von Wissen an die neue Generation von Arbeitnehmer:innen, die den Sektor übernehmen werden, wird die Einführung neuer Technologien gesehen: Die Schaffung digitaler Wissensspeicher wird die Ausbildung neuer Arbeitskräfte erleichtern und im Gegenzug zur Entwicklung datengesteuerter Systeme führen, die auf der Erfahrung von Generationen von Expert:innen und lokalen Arbeitskräften aufbauen.

Ziel und Aufbau des Berichts

Digitale Technologien sind zwar für die Bewältigung der künftigen Herausforderungen in der städtischen Wasserwirtschaft von grundlegender Bedeutung, doch die Einführung vernetzter und integrierter digitaler Lösungen schafft neue Probleme für die Cybersicherheit. Insbesondere die zunehmende Automatisierung des Wassersektors eröffnet neue

Angriffsflächen für böswillige Cyberaktivitäten.

Dieser Bericht zielt darauf ab, **die mit der Digitalisierung des Wassersektors verbundenen Trends darzustellen und die damit einhergehenden Cyberrisiken zu beleuchten**. Es geht weniger darum, die aktuelle Cybersicherheitslage zu beschreiben oder die Defizite und den Umsetzungsbedarf auf technischer und organisatorischer Ebene im Detail zu erläutern. Stattdessen soll der Bericht das derzeitige Wissen der Betreiber ergänzen und aufzeigen, welche neu entstehenden Risiken die Betreiber im Zuge der digitalen Transformation in Zukunft berücksichtigen müssen.

Zunächst wird ein Überblick über die Schlüsselelemente des Wasser 4.0 gegeben, die sich in den letzten Jahren herausgebildet haben und die künftige Praktiken in der städtischen Wasserwirtschaft beeinflussen und prägen dürften **(Kapitel 1)**. Auf der Grundlage von fünf identifizierten Trends (**IoT und Intelligente Sensoren**, **KI für die Wasserwirtschaft**, **Cloud-Migration**, **Transformation der Infrastruktur** und **Smart Cities**) wird ein tieferes Verständnis der Treiber und des Potenzials der digitalen Revolution anhand konkreter Umsetzungsbeispiele bei führenden Betreibern vermittelt **(Kapitel 2)**. Nach der Entwicklung der Trends konzentriert sich der Bericht auf die Analyse der wichtigsten Arten von Risiken, die mit der digitalen Transformation verbunden sind, und gibt einen Überblick über neue Risiken, die immer wichtiger werden könnten **(Kapitel 2)**. Da die laufende Transformation nicht nur Wasserbetreiber betrifft, werden auch Innovationen, Herausforderungen und Bedenken aus anderen Sektoren hervorgehoben und es wird versucht zu verstehen, wie die Erfahrungen anderer kritischer Infrastrukturen für den Wassersektor von Nutzen sein könnten.

Schließlich baut der Bericht auf den identifizierten Trends und neuen Risiken im Zusammenhang mit der Digitalisierung des Wassersektors auf, um 14 konkrete Forschungs- und Entwicklungsbedarfe aufzuzeigen **(Kapitel 3)**. Wir hoffen, dass diese Perspektiven die Betreiber und den gesamten Wassersektor auf ihrem Weg zu widerstandsfähigeren und cyber-sicheren Wasserinfrastrukturen unterstützen werden.

Während der Vorbereitung dieses Berichts wurden Interviews mit zehn Vertreter:innen des Wassersektors (hauptsächlich Betreiber, Forscher:innen und Beratungsunternehmen) geführt. Sie wurden zu den zukünftigen Entwicklungen und den Cybersicherheitsrisiken und -maßnahmen der fünf identifizierten Trends der Wasserinfrasktur sowie zu übergreifenden Management- und Weiterbildungsansätzen befragt. Um die Vertraulichkeit der Befragten zu wahren, wurden die Ergebnisse verwendet, um unsere Erkenntnisse aus der Literatur zu ergänzen, zu bestätigen und zu konsolidieren oder um einige in der Literatur weniger diskutierte Elemente hervorzuheben.

Die Vision für die Zukunft

Abbildung 1 gibt einen grafischen Überblick über die Schlüsselelemente des Wasser 4.0, die sich in den letzten Jahren herausgebildet haben und künftige Praktiken der städtischen Wasserwirtschaft beeinflussen und prägen werden. Aus diesem Diagramm lassen sich die wichtigsten Trends ablesen, die zur weiteren Strukturierung dieses Berichts und zur Ableitung der damit verbundenen Risiken in Kapitel 2 herangezogen werden.

Dieses Diagramm kann sequentiell verstanden werden, beginnend von unten, wo neue Echtzeitinformationen durch intelligente Sensoren, intelligente Zähler und Internet of Things (IoT)-Technologien erzeugt werden. Daten sind das neue Gold und bilden das Rückgrat der Betreiber, um die Überwachung, das Verständnis und die Kontrolle von Infrastrukturen und Ressourcen zu unterstützen **(Trend 1: IoT und intelligente Sensoren)**. Diese Revolution kommt nicht ohne Herausforderungen aus, da die Betreiber mit großen Mengen heterogener Daten aus verschiedenen Quellen, einschließlich strukturierter, halbstrukturierter und unstrukturierter Daten umgehen müssen. Wenn man bedenkt, dass strukturierte Daten (typische tabellarische Daten, die in Tabellenkalkulationen oder Datenbanken zu finden sind) nur 5 % aller vorhandenen Daten ausmachen (Cukier 2010), besteht die Herausforderung darin, die strukturelle Vielfalt der Daten, einschließlich Text, Bilder, Audio und Video, die von einer Reihe von Datenproduzenten und auch von Bürger:innen erzeugt werden, nutzbar zu machen (Gandomi et al. 2015). Die weite Verbreitung von Geräten, die Daten in hoher Auflösung und Häufigkeit erzeugen (z. B. kostengünstige Sensoren, Smartphones, soziale Medien), birgt für Betreiber das Risiko, von Daten überflutet zu werden, und stellt sie vor die Herausforderung, diese in ein wertvolles Produkt umzuwandeln (Ornes 2013).

Hier kommen Modellierungslösungen und vor allem KI ins Spiel **(Trend 2: KI für die Wasserwirtschaft)**. KI hat die Fähigkeit, mittels Algorithmen aus Daten jeglicher Form, natürliche Sprache, Bilder und Muster zu erkennen (Kumar et al. 2016). Sie ist in der Lage, Daten zu interpretieren, von ihnen zu lernen und diese Erkenntnisse zu nutzen, um bestimmte Ziele und Aufgaben zu erreichen (Kaplan und Haenlein 2019). Insbesondere wird erwartet, dass das maschinelle Lernen, das als Teil der künstlichen Intelligenz betrachtet wird, eine größere Rolle bei der Verwaltung der Wasserinfrastruktur spielen wird. Denn maschinelles Lernen ist in der Lage, die verfügbaren Daten zu nutzen, um zu lernen und das aktuelle oder zukünftige Verhalten von Systemen vorherzusagen.

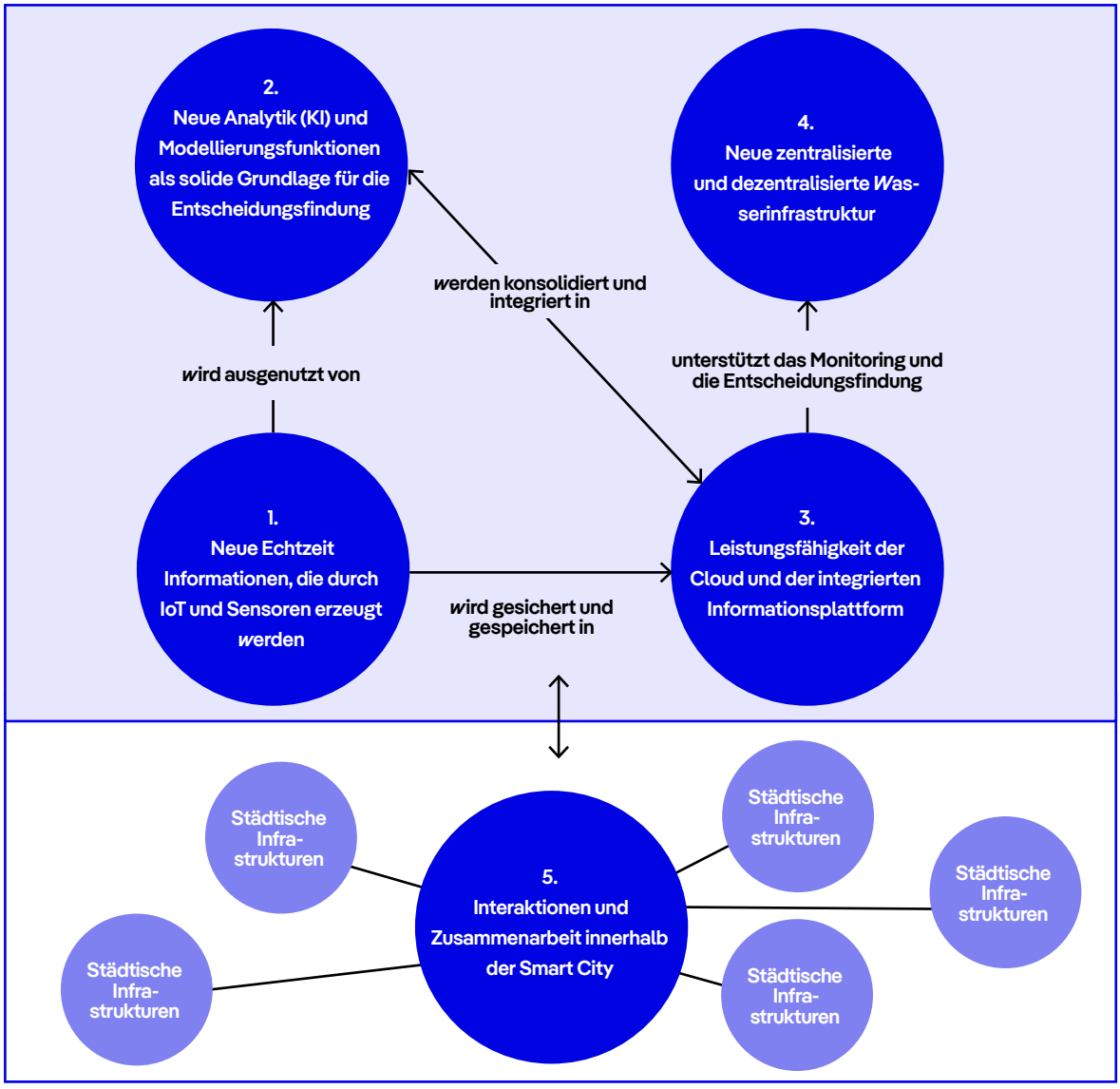


Abbildung 1
Schlüsselelemente des Wasser 4.0 und ihre Interaktion (angepasst nach Makropoulos und Savić 2019)

Im Vergleich zu herkömmlichen Modellierungsansätzen in diesem Bereich führt das maschinelle Lernen zu einer flexiblen mathematischen Struktur, die in der Lage ist, nichtlineare und komplexe Beziehungen zwischen Eingabe- und Ausgabedaten zu erkennen (Ahmed et al. 2019). Maschinelles Lernen leistet einen Beitrag dazu, Daten in Wert zu setzen und den Betreibern somit neue Planungskapazitäten zur Verfügung zu stellen, z. B. zur Vorhersage des Wasserbedarfs und -verbrauchs, zur Umsetzung vorausschauender Wartungsstrategien oder zur Entwicklung digitaler Zwillinge unserer Infrastrukturen (Mehmood et al. 2020). Durch Verstärkungslernen werden sich die Modelle auch weiterentwickeln, anpassen und aus ihren Fehlern lernen, um die Steuerung dynamischer Systeme zu verbessern (Martinez-Piazuelo et al. 2020).

Der zunehmende Einsatz von IoT- und Modellierungstools geht mit dem Aufkommen von Cloud-Lösungen und Software-as-a-Service (SaaS) einher, die voraussichtlich zur gängigen Praxis werden **(Trend 3: Cloud-Migration)**. Ab 2021 werden rund 50 % aller Unternehmensdaten in der Cloud gespeichert sein. Im Jahr 2015 lag dieser Anteil erst bei 30 % und wächst weiter, da Unternehmen ihre Ressourcen zunehmend in Cloud-Umgebungen verlagern (Statista 2022). Cloud-Lösungen bieten die Skalierbarkeit, die Betreiber benötigen, um die riesige Menge an generierten Daten zu verarbeiten und zu speichern. Sie bieten aber auch die Rechenleistung, die erforderlich ist, um den gesamten Lebenszyklus der Daten von der Produktion bis zur Entscheidungsfindung zu verarbeiten. In Europa zielen neue Plattformen wie Gaia-X genau darauf ab, das Rückgrat dieses Wandels zu sein, indem sie den Rahmen für eine standardisierte Cloud-Netzwerkinfrastruktur schaffen (Gaia-X 2021). Gemeinsame Standards für die Interoperabilität sind der Schlüssel zur Gewährleistung der Anpassungsfähigkeit von Lösungen (z. B. an neue Nutzeranforderungen) und zur Förderung der Entwicklung digitaler Lösungen, die leicht übertragbar und städteübergreifend replizierbar sind. Die Interoperabilität wird auch auf europäischer Ebene als zentrale Herausforderung gesehen. Ziel ist es, Eintrittsbarrieren sowie die Bindung an spezifische Anbieter (Vendor Lock-in) zu vermeiden und die Entwicklung offener Schnittstellen zu fördern, die mit der Mehrzahl der bestehenden Systeme kompatibel sind (ICT4Water 2018).

Diese neue Technologielandschaft bietet den Betreibern neue Instrumente, Optionen und Szenarien zur Verbesserung der Planung und des Managements von Wassersystemen sowie zur Gestaltung der klimagerechten Entwicklung der städtischen Wasserinfrastruktur **(Trend 4: Transformation der Infrastruktur)**. Die vernetzte Infrastruktur, die derzeit in den meisten europäischen Städten zur Bewirtschaftung der Wasserversorgung und Abwasserentsorgung genutzt wird, wurde vor über 100 Jahren eingerichtet. Rückblickend waren diese Infrastrukturen und die mit ihrem Betrieb betrauten Organisationen bei der Erreichung von Entwicklungs- und Sanierungszielen sehr erfolgreich (zumindest in Ländern mit hohem Einkommen). Heute wird ihre Wirksamkeit bei der Erfüllung von Umwelt-, Lebensqualitäts- und einer Reihe anderer Ziele auf lange Sicht oft in Frage gestellt (Knieper und Pahl-Wostl 2016). Alternde Infrastrukturen, zunehmende Verstädterung und neu auftretende Schadstoffe sind nur einige der Faktoren, die die wirtschaftlichen, sozialen und ökologischen Kosten erhöhen, selbst in Ländern mit einer langen Tradition erfolgreicher Praktiken (Larsen et al. 2016). Zugegebenermaßen kann die Zukunft des urbanen Wassermanagements nicht nur in der Digitalisierung der bestehenden Anlagen und der Beibehaltung der traditionellen Infrastruktur, Finanzmechanismen und Governance-Formen bestehen. Die Betreiber müssen kostengünstigere und ressourceneffizientere Systeme entwickeln, die die gewünschten Wasserdienstleistungen ohne die einschränkenden Zwänge des herkömmlichen zentralisierten Systems erbringen. Die Notwendigkeit eines „Paradigmenwechsels“ (Knieper und Pahl-Wostl 2016) wird für die Regenwasserbewirtschaftung klar erkannt: Nachhaltige Stadtentwässerungssysteme (SUDS) und naturbasierte Lösungen (NBS) zielen darauf ab, einen natürlicheren Wasserkreislauf im Herzen der Städte wiederherzustellen und setzen auf eine starke Dezentralisierung der Elemente. Im Hinblick auf die Ressourcen entstehen neue Ansätze zur Verbesserung der „Wasserproduktivität“, z. B. durch die Reduktion und Wiederverwendung von Abwasser (Grant et al. 2012). Auf der Ebene der Haushalte wird die Trennung von Abwasserströmen ebenfalls als vielversprechende Option angesehen, um die Rückgewinnung von Ressourcen zu fördern, den Behandlungsprozess zu erleichtern und die Wiederverwendung von Wasser auf dezentraler Ebene zu ermöglichen. Die Urinseparierung ist noch immer keine selbstverständliche Alternative zum konventionellen zentralen System. Sie zeigt aber vielversprechende Perspektiven auf, z. B. für die Wasserbewirtschaftung in informellen Siedlungen in Entwicklungsländern, in denen starke Sanitärprobleme von einem Mangel an konventioneller zentraler Infrastruktur verschärft werden (Larsen et al. 2021). Zentrale Systeme können nicht von heute auf Morgen voll-

ständig ersetzt werden, aber es gibt jetzt Alternativen für die lokale Wasserversorgung und -aufbereitung, die den Wandel der Infrastruktur hin zu einer „extremen Dezentralisierung“ beschleunigen (siehe das von Rabaey et al. 2020 geprägte Konzept des „Dritten Weges“).

Wir haben gesehen, dass Wassersysteme in einem kontinuierlichen Wandel stehen; es überrascht uns nicht, dass auch die Städte tiefgreifende Veränderungen durchlaufen **(Trends 5: Smart City und die neue Rolle des Wassers)**. Die Vision der intelligenten Städte (Smart Cities) prägt die Zukunft der städtischen Gebiete: sicher, lebenswert, nachhaltig und effizient, wo öffentliche Infrastrukturen, Dienstleistungen und Verwaltung (z. B. Wasser, Abwasser, Energie, Verkehr, Stadtplanung, usw.) durch den Einsatz digitaler Lösungen und Plattformen miteinander verbunden sind (Hall et al. 2000). In den letzten Jahrzehnten haben die Betreiber ihre eigenen Dienste digitalisiert, was zur Verbreitung von in sich geschlossenen Anwendungen (oft als „Silos“ bezeichnet) führte, die Dienste mit starker vertikaler Integration anbieten (Frascella et al. 2018). Das Ergebnis ist ein Mangel an horizontalen Datenflüssen zwischen vertikalen Anwendungen bei Betreibern, der Stadtverwaltung und den Bürger:innen. Kurz gesagt, es fehlt an Interoperabilität zwischen Anwendungen. Bisher sind die Anwendungen zwar in der Lage, Daten vom Feld bis zu den Entscheidungsunterstützungssystemen zu verarbeiten, sie sind jedoch nicht in der Lage, mit anderen Systemen zu interagieren (Brutti et al. 2019). Die Stadt der Zukunft zielt darauf ab, diese Silos aufzubrechen und Daten aus verschiedenen Bereichen zu nutzen, um datengestützte Entscheidungen zu treffen, unseren ökologischen Fußabdruck zu verringern und das Engagement der Bürger:innen zu fördern. Welche Rolle wird die Wasserwirtschaft in dieser neuen Konstellation spielen? Wie werden die Wasserversorger das Potenzial einer Vielzahl von Datenquellen nutzen, die von anderen Betreibern oder Bürger:innen generiert werden? Dies sind Fragen, mit denen sich die Betreiber in Zukunft auseinandersetzen müssen, um die Rolle der Wasserwirtschaft in der intelligenten Stadt zu gestalten.

Die dargestellten Trends geben einen Eindruck von den immensen Herausforderungen, die die Betreiber auf ihrem Weg hin zur Digitalisierung erwarten. Mit der Durchdringung von Wirtschaft und Gesellschaft durch die digitale Technologie steigt jedoch auch deren Anfälligkeit (Almeida et al. 2020). Dies trifft auch auf den Wassersektor zu, denn eine zunehmende Vernetzung und Automatisierung birgt die Gefahr, dass böswillige Cyber-Aktivitäten Dienstleistungen stören oder manipulieren könnten (Montgomery und Logan 2021). Im nächsten Kapitel werden die oben dargestellten Trends untersucht und die wichtigsten Cyberrisiken im Zusammenhang mit diesen Veränderungen aufgezeigt.

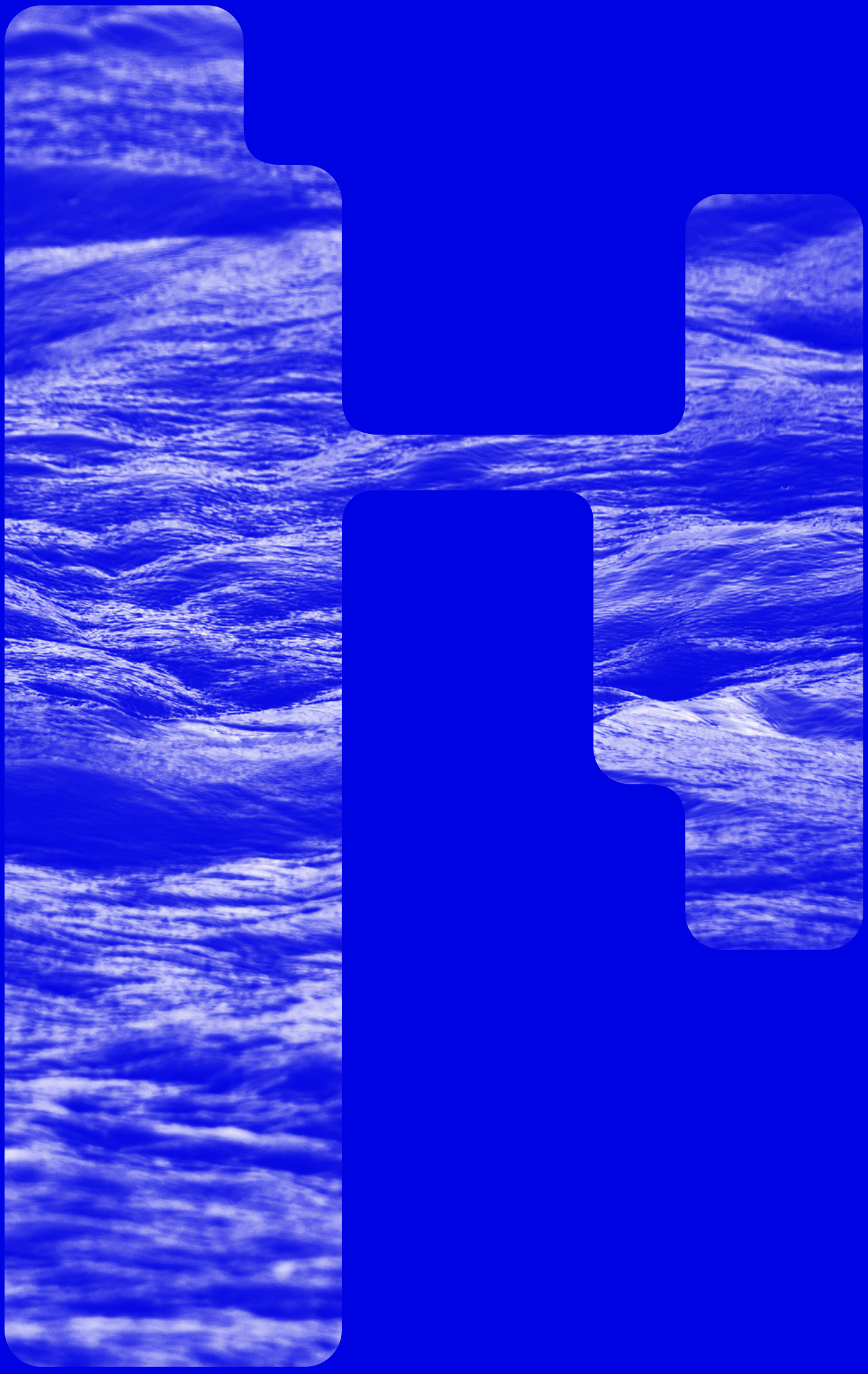
Für ein besseres Verständnis des aktuellen Stands der zunehmenden Digitalisierung des Wassersektors

Makropoulos, C., & Savić, D. A. (2019) Urban hydroinformatics: past, present and future. Water, 11 (10): 1959.

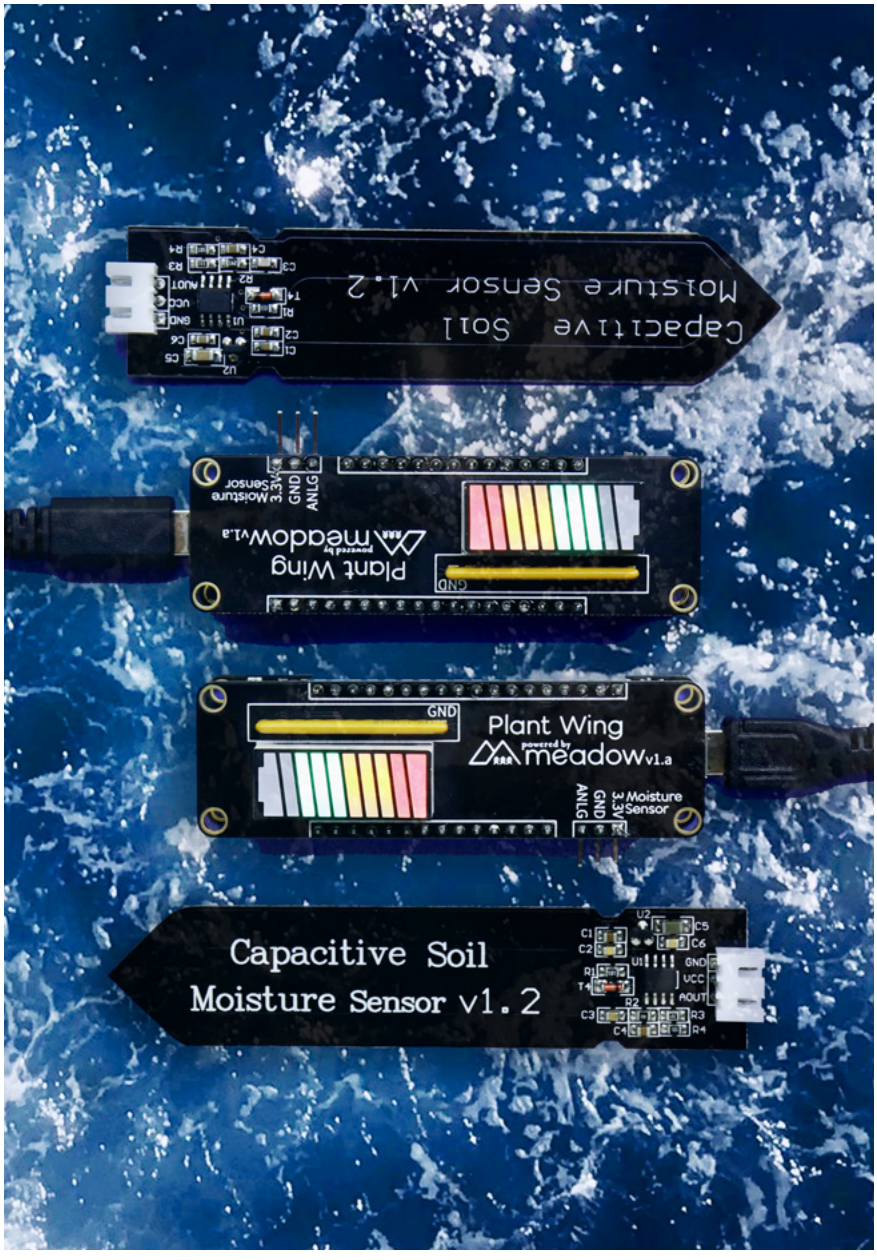
Zukünftige Entwicklung

Im folgenden Kapitel werden die fünf identifizierten Bereiche des Wasser 4.0 hinsichtlich ihrer Haupttrends näher analysiert. Die digitale Transformation des Wassersektors bietet enorme Chancen, birgt jedoch auch beachtliche Risiken. Dieses Kapitel zielt darauf, die Komplexitäten aufzudecken und dabei Innovationen, Herausforderungen sowie Bedenken aus anderen Sektoren mit einzubeziehen.

Inhalt



IoT und Sensorik



Werden die aktuellen Praktiken des Wassermanagements bis 2050 beibehalten, stehen ca. 63 Trillionen US-Dollar bzw. 45 % des zu dem Zeitpunkt voraussichtlichen globalen BIP auf dem Spiel (International Food Policy Research Institute in Sarni et al. 2018). Daher wird ein akuter Wandel der Wasserinfrastruktur in Richtung transparenter, nachhaltiger und effizienterer Netzwerke benötigt. Diese digitale Revolution des Wassersektors beruht auf Sensorik, Kommunikationsnetzen und Cloud-Infrastrukturen, wodurch das Konzept des Internet of Things realisiert werden kann. Das IoT beschreibt eine Umgebung, in der jedes Objekt miteinander kommuniziert. So können in der Wasserinfrastruktur die Präzision von Prozessen erhöht, die Automatisierung der Anlagen verstärkt und die Kosten der Unterhaltung gesenkt werden (Boyes et al. 2018).

Für einen Überblick zu aktuellen IoT Anwendungen des Wasserqualitätsmonitoring

Jan, F. et al. (2021) Iot based smart water quality monitoring: Recent techniques, trends and challenges for domestic applications. Water 13 (13): 1729.

Das IoT fügt sich aus vier Ebenen zusammen: die Sensorkomponenten an unterster Stelle, anschließend die Gatewaykomponenten und Datenübertragungsnetzwerke, darüber die Datenverarbeitungsinfrastruktur (die Cloud) und zuletzt die Anwendungsebene (Baanu und Babu 2021, Jan et al. 2021). Neben der Verschärfung analytischer Prozesse und der Ermöglichung von Echtzeit-Anwendungen, bietet das IoT vielfältige Vorteile. Dazu zählen die vergleichsweise niedrigen Unterhaltungskosten (aufgrund der kostengünstigen und verbrauchsarmen Sensoren und Kommunikationsnetzwerke) und die autonome Wirkungsweise, die ohne menschliches Zutun auskommt. Zudem ist durch die Verbindung zur Cloud die Speicherkapazität theoretisch unbegrenzt und die Rechenfähigkeit kann ausgelagert werden (Jan et al. 2021).

Im Energiesektor werden IoT-Ansätze angewendet, um das Monitoring sowie die Instandhaltung der Anlagen zu verbessern und somit Ausfälle zu reduzieren. Durch die Einbettung von intelligenten Sensoren kann das Asset Management viel effizienter ausgeführt werden. Mit einer IoT-Plattform ausgestattete Kraftwerke können somit zwischen 50 Millionen US-Dollar (für bereits existierende) und 230 Millionen US-Dollar (für neu gebaute Kraftwerke) Kosten einsparen (Motlagh et al. 2020). IoT-Technologie ist auch für die Optimierung des Verhältnisses zwischen Energiebedarf und -erzeugung vorteilhaft, da durch die erhöhten Datenmengen z. B. die Variabilität von erneuerbaren Energiequellen ausbalanciert werden kann.

IoT-Ansätze für den Wassersektor

Das IoT ermöglicht es, durch ein automatisches System-Monitoring die Wasserversorgung zu sichern, die Wasserqualität zu verbessern und den Wasser- und Energieverbrauch zu reduzieren (Koo et al. 2015). Gleichzeitig trägt eine IoT-Infrastruktur zur Reduktion der benötigten Zeit, Kosten und Arbeitskräfte im Vergleich zu herkömmlichen Analysen bei (Baanu und Babu 2021). Da Analysen im IoT in Echtzeit verlaufen, wird auch die Geschwindigkeit von Prozessen der Wasserinfrastruktur erhöht (Sarni et al. 2018). IoT-Systeme können zudem relativ einfach hochskaliert werden und benötigen, dank weitverbreiteter Kommunikationsprotokolle, geringe Konfigurierung (Singh und Ahmed 2021).

Hieraus lassen sich Ansätze für die weitere Entwicklung der auf Sensoren basierenden Prozesse des Wassersektors ableiten.

IoT für Gewässermonitoring

Monitoringsysteme bestehen aus einfachen Sensoren (die am häufigsten angewendeten dienen der Messung von Ultraschall, Temperatur, pH, Trübheit, Salzgehalt und gelöstem Sauerstoff), einem Microcontroller (oft Arduino Unos oder bei höherer Komplexität ein Raspberry Pi) und einer Cloudanwendung (wie Thingspeak oder Freeboard) (vgl. Xiaocong et al. 2015, Rao et al. 2018, Kulkarni et al. 2020, Singh und Ahmed 2021). Zum Beispiel haben Chowdury, Emran et al. (2019) ein Monitoringsystem zur Messung der Flusswasserqualität entwickelt, das mittels einer IoT-Plattform in Echtzeit Daten aufnimmt und auswertet. Gegenüber herkömmlichen Systemen bietet die IoT-Infrastruktur eine deutlich erhöhte Zuverlässigkeit, Skalierbarkeit, Geschwindigkeit und Langlebigkeit.

IoT für Irrigationssysteme

Die Agrarwirtschaft verbraucht in Europa 36 % des gesamten jährlichen Wasserverbrauchs (Compagnucci und Spigarelli 2018). Im Vergleich zu herkömmlichen Irrigationssystemen können intelligen-

te IoT-Systeme, bis zu 70 % Wasser einsparen (Ismail et al. 2019). Auf Basis eines IoT-Sensorennetzwerks können Messwerte zur Luftfeuchtigkeit, Bodenfeuchtigkeit, Temperatur und Druck kontinuierlich und in Echtzeit aufgenommen und an eine Cloud geschickt werden. Dort können sie verarbeitet und visualisiert sowie zur Steuerung eines intelligenten Bewässerungssystems über eine Android-App weitergenutzt werden. Dank des Einsatzes von IoT-Technologien können hier mit niedrigen Umsetzungskosten der Wasserverbrauch, die Arbeitskraft und der Energieverbrauch reduziert und die Verlässlichkeit erhöht werden (Ismail et al. 2019).

IoT für Überflutungskontrollsysteme

Mit dem fortschreitenden Klimawandel werden Extremwetterereignisse und Überflutungen zunehmend stattfinden. Um die öffentliche Sicherheit zu fördern und die durch Überflutungsereignisse verursachten Infrastrukturschäden zu verringern, sind Überflutungskontrollsysteme für die Vorhersage oder gar Vorbeugung von solchen Katastrophen essenziell. Dank der Fortschritte des IoT kann die Geschwindigkeit und Genauigkeit solcher Prozesse verbessert werden. Ein Anwendungsbeispiel ist das von ENVIRA IoT entwickelte Hochwasserüberwachungs- und -warnsystem. Durch den Einsatz der IoT-Architektur schafft das ENVIRA IoT System eine Echtzeit-Fernüberwachung von Wasserwegen und klimatischen Gegebenheiten. Diese werden automatisch an eine Cloud-Infrastruktur weitergeleitet, um die Daten zu visualisieren und auszuwerten. Anhand eines Dashboards können Nutzer:innen den Zustand und die Historie jeder Messstation einsehen. Über integrierte ML-Systeme können Risiken vorhergesagt und Warnungsmeldungen per SMS oder E-Mail an Verantwortliche weitergeleitet werden. Die IoT-Umgebung erlaubt nicht nur eine erhöhte Messgenauigkeit und eine Datenübertragung in Echtzeit, sondern ermöglicht es auch auf einfacher Weise die Datenumgebung in Bezug auf Menge, aber auch Art von Sensoren zu erweitern und die erhobenen Datensätze direkt in weitere Anwendungen einzuspeisen (ENVIRAIoT o. J.).

IoT für Trinkwassernetzte

Eine Anwendungstypologie, die durch das IoT ermöglicht wird, ist der Smart Water Grid, ein Versorgungsnetz, in dem ein bidirektionaler Informationsfluss vorliegt und welches ursprünglich aus dem Energiesektor stammt. Dadurch können ein zeitunabhängiges, dauerhaftes Ablesen des Verbrauchs aus der Ferne sowie Wasserbedarfsanalysen und -prognosen vorgenommen werden. Zudem kann ggf. auch eine Fernsteuerung ermöglicht werden. Dies kann durch das An- und Ausschalten von Netzkomponenten zur Cyber- und physischen Sicherheit beitragen (Müller 2011, Brem 2021). Beispielsweise wurde ein neuer Trinkwasserzähler von Gelsenwasser, der physec GmbH und Kampstrup, zum leichteren Ablesen und Sammeln von Verbrauchsinformationen sowie zur verbesserten Übersicht des Versorgungsnetzes entwickelt und aktuell in Gelsenkirchen getestet. Gleichzeitig können, über den bidirektionalen Informationsfluss, Verbraucher:innen ihre Verbrauchsdaten einsehen und über den Zustand ihrer Hausinstallation informiert werden (Gelsenwasser 2020).

Für eine Befragung von IoT Expert:innen zur Entwicklung von Risiken

Tanczer, L. M. et al. (2018) Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? Living in the Internet of Things: Cybersecurity of the IoT-2018, IET.

Erweiterungen des IoT mit Blockchain

Außerhalb von Monitoring- und Managementsystemen kann das Konzept und die Architektur des IoT auf weitere Arten von Anwendungen ausgeweitet werden und sowohl zur Etablierung neuer infrastrukturellen als auch organisatorischen Paradigmen beitragen. Ein gutes Beispiel für diesen Ansatz ist die Nutzung der Blockchain-Technologie für IoT-Netzwerke. Hier liegen die Vorteile in einer Erhöhung der Transparenz, Sicherheit und Effizienz verschiedener transaktionsbezogener Prozesse des smarten Wassermanagements, wie z. B. die dezentralisierte Finanzierung von Anlagen oder die Unterstützung eines virtuellen (internationalen) Wasserhandels (Dogo et al. 2019). Aufgrund ihrer digitalen Eigenschaft können nationale Währungsfluktuationen umgangen und durch die Grundprinzipien der Blockchain (als peer-to-peer distributed ledger mit hashing-Funktionen) die oben genannten Vorteile bei Transaktionen gewährleistet werden (Sarni et al. 2018).

Das Water Credits Projekt von Smart4tech ist auf einer Blockchain-Plattform aufgebaut und hat das Ziel, die Nachhaltigkeit des gesamten Sektors zu stärken. Abhängig von Einflussfaktoren, die positiv auf eine umweltverträgliche Wasserwirtschaft zielen, werden finanzielle Anreize für betei-

ligte Stakeholder geschaffen. Die Vorschriftseinhaltung, Innovation und Kooperation der beteiligten privaten und öffentlichen Akteure können auf transparente und sichere Weise anhand der Blockchain mit Credits, die auf einem (digitalen) Marktplatz ausgetauscht werden können, belohnt werden (Poberezhna 2018).

Das Weltwirtschaftsforum sieht in der Einbettung von Blockchain aufgrund der sich dadurch verändernden Risikoprofile eine Erhöhung der Investitionsattraktivität bei kleineren Betreibern. Ein Grund dafür wird in den sog. smart contracts gesehen, die es ermöglichen, auf einfache Weise mehrere hundert Investoren einzubeziehen.

Blockchain-Technologien können ebenfalls, aufgrund ihrer natürlichen Eigenschaften, bestimmte Sicherheitslücken des IoT decken, besonders in Bezug auf Datenmanipulation (Mahmoud et al. 2019). Im Zuge der fortschreitenden Digitalisierung und wachsenden Cyberangriffe wird dies in Zukunft an Bedeutung gewinnen.

Die Sensorik der Zukunft: Anwendungsbereiche und Potenzial

Die Fortschritte der IoT und deren Anwendungen sind in erster Linie von ihrem Grundbaustein, dem Sensor, abhängig. Intelligente Sensoren, die als Teil von Sensornetzwerken ihre Daten in Echtzeit übertragen können, sind der Ausgangspunkt für die oben genannten komplexen Anwendungen und werden sich auch zukünftig weiterentwickeln, um diese in ihrer Tiefe und Breite zu erweitern. Sensoren entwickeln sich hin zu kostengünstigen, kompakten, verbrauchsarmen und umfassenden Komponenten. Zudem werden kabellose Ansätze stärker vertreten sein, um die Einsatzmöglichkeiten und Resilienz dieser zu erhöhen (Bock et al. 2018).

Wasserqualitätssensoren

Neue Generationen von Sensoren werden entwickelt, um die Einschränkungen der derzeitigen Anwendungen zu überwinden, wie z. B. der hohe Wartungsbedarf oder die schlechte Leistung der Sensoren unter schwierigen Bedingungen in Kanalnetzen. Zum Beispiel wird in Schweden ein innovativer Trübheitssensor entwickelt, der über Laserstrahlen und eine Kamera die Trübheit im Wasser ohne direkten Kontakt messen kann (Göteborg 2020, Galfi 2022).

Sensorinnovationen finden auch in Bezug auf die physische Beschaffenheit der eingesetzten Materialien statt, da durch die Skalierung auf Nano-Ebene einzigartige optische, elektrische oder magnetische Eigenschaften entstehen, anhand derer eine erhöhte Genauigkeit der Messverfahren ermöglicht wird. Nanosensoren liegen bereits für Mikroorganismen (Cryptosporidium, Giardia lamblia, Legionella, E. Coli und bestimmte Viren), anorganische Chemikalien (außer Asbest, Barium, Beryllium und Bor) und verschiedene organische Chemikalien sowie für Nebenprodukte der Desinfektion vor. Nanosensoren eignen sich für das Monitoring von Trinkwassernetzen, besonders beim Einsatz von recyceltem Wasser und für dezentralisierte Anlagen. Für einen verbreiteten Einsatz bedarf es jedoch noch weiterer Recherche (Vikesland 2018). Vielversprechende Anwendungen sind auch die Verwendung von Nanomaterialien auf Graphen-Basis für den elektrochemischen Nachweis von Nitrat, Nitrit (Wang et al. 2020) oder Schwermetallen (Chang et al. 2014) im Wasser. Die spezifischen Eigenschaften von Kohlenstoff-Nanomaterialien könnten zu neuartigen, kostengünstigen Sensoren mit höherer Genauigkeit führen.

Remote Sensing

Die Möglichkeiten der Fernerkundung sind bereits gut bekannt und eignen sich für das Monitoring von Niederschlag, Wasserhaushalt und Wasserqualität auf regionaler Ebene. So können beispielsweise Satelliten oder Drohnen die Wasserressourcen anhand von Bildern genau kartieren und die Wasserqualität und -dynamik überwachen (Chastain-Howley 2018, Schlaman und Smal 2018, Sarni et al. 2019). Neue Perspektiven für den Einsatz dieser Technologie ergeben sich auch im städtischen Kontext. Innovationen in satellitenbasierte optische Fernsensoren, wie z. B. Verfahren zur Auflösungsannäherung oder Algorithmen zur Verringerung von Interferenzen aufgrund von Wolken oder Vegetation, führen dazu, dass Abschätzungen zu Dynamiken von Oberflächengewässern effizienter und mit erhöhter Genauigkeit durchgeführt werden können (Huang et al. 2018). Zudem können anhand von multispektralen Satellitenbildern auch städtische Gewässer überwacht und im Vergleich zu herkömmlichen Methoden schnellere und genauere Ergebnisse produziert werden (Chen et al. 2018, Chen et al. 2020). Eine weitere vielversprechende Entwicklung ist der Einsatz von Drohnen zur Messung der Wasserqualität, entweder durch die Erfassung von Daten mit Sonden oder durch die physische Entnahme von Wasserproben (Alam und Manoharan 2016). Die Möglichkeit, mehrere Standorte in der Stadt schnell und effizient direkt zu überwachen, würde den

Betreibern verwertbare Daten liefern, die helfen könnten, die Ressourcenbeschränkungen von klassischen Messkampagnen zu überwinden (McDonald 2019).

Asset Management und Zustandsbewertung

Ein weiteres Beispiel zur maschinengestützten Erhebung von Messwerten sind Roboter und Drohnen, die Kanaldaten sammeln und aufgrund ihrer besonderen Einsatzbereitschaft, Robustheit und Effizienz in Zukunft vermehrt eingesetzt werden (Savić 2021). Flyability und Flind haben in Barcelona Drohnen eingesetzt, um den genauen Zustand des Kanals einzusehen. Laut Flind sind Einsätze mit Drohnen rund 40 % kostengünstiger und doppelt so effizient wie die menschlicher Kanalbefahrer:innen (Flyability o. J.). Das Unternehmen WinCan ist vor Kurzem eine Partnerschaft mit Flyability eingegangen, um Drohnendaten in ihre Kanalinspektionssoftware zu importieren. Auf diese Wiese soll eine automatische Zustandsbewertung der untersuchten Kanäle ermöglicht werden (Flyability 2022). Pipebots, eine Partnerschaft verschiedener englischer Universitäten, entwickeln autonome Roboter zur Kanalinspektion. Neben der Fähigkeit zu laufen und zu schwimmen, haben die Roboter integrierte Sensoren und Kameras, um ihre Umgebung zu erkunden und Defekte im Kanalnetz zu erkennen. Die gescannten Informationen werden kabellos an Ingenieur:innen weitergeleitet, die die genaue Lage des Rohrbruchs in der Infrastruktur über eine Netzsimulation einsehen und entsprechend reagieren können (Pipebots 2021). Solche Entwicklungen sind sehr vielversprechend für die Weiterentwicklung der Instandhaltungspraxis. Mit den richtigen Innovationen wäre eine neue Generation von Drohnen in der Lage, autonom in unseren Kanalisationsnetzen zu fliegen und ständig aktualisierte Informationen über den Zustand der unterirdischen Infrastrukturen zu liefern.

Citizen Science

Um die logistische Herausforderung der Umsetzung des IoT zu begegnen und Datenlücken zu füllen, können Citizen Sensing-Maßnahmen angewendet werden. Diese Maßnahmen tragen unter niedrigeren Kosten zur Erhöhung der Anzahl an Messstellen bei und schaffen gleichzeitig, dass Bürger:innen ein Bewusstsein für nachhaltiges Wassermanagement entwickeln. Durch die Entwicklung und Verteilung von Citizen Sensing Kits wird eine neue Dimension des IoT aktiviert, die zur Produktion von neuen granularen Datensätzen, einen verbesserten Übergang von Theorie zu Praxis und eine stärkere Wassergovernance führt (Fab Lab Barcelona o. J., Paul und Buytaert 2018, Capdevila et al. 2020).

Prozessinnovationen der Sensorik

Neben neuen Anwendungsbereichen werden sich auch die Funktionen der Sensoren in Zukunft weiterentwickeln.

Autonomes Handeln z. B. durch frühzeitige Konfiguration und Folgenabschätzung

Das RemoteStream Projekt an der Uni Aberdeen hat einen Sensor samt Wireless Sensing Network (WSN) entwickelt, das autonome Überwachungen und ein eigenes Energiemanagement durchführen kann. Beispielsweise wurde es im Katastrophenschutz und im Wasservorratsmonitoring angewendet. Letzteres geschah in Partnerschaft mit UNICEF im Sudan in Form einer Brunnenüberwachungs- und Pumpoptimierungsanwendung: Die Position der Pumpe passte sich an die Wassermenge, also saisonalen Fluktuationen und Nutzverhalten, an und leitete diese Daten zur Auswertung von Migrationsflüssen weiter (Nazir et al. 2015).

Selbstüberwachung und -konfiguration

Um die Heterogenität von IoT-Komponenten zu begegnen, haben Ayala et al. die Sol Agentenplattform entwickelt, die als Gateway zwischen unterschiedlichen Kommunikationsprotokollen dient. Die Agenten können derweil ihre interne Architektur selbst konfigurieren, um sich den kontextuellen Kommunikationsprotokollen anzupassen (Ayala et al. 2015).

Energieautarkie

Um eine dauerhafte Datenübertragung der Sensoren zu gewährleisten, kann Energy Harvesting angewandt werden. So kann aus natürlichen Quellen Energie gewonnen werden, wie z. B.
aus Solar- oder thermischer Energie oder aus Energiequellen „künstlichen“ Ursprungs, wie Druck oder Vibration (Adu-Manu et al. 2017, Dzombak et. al. 2012).

In den Stadtwerken Winterthur wurden Smart Water Pipes installiert. Diese sind mit komplett autarken Sensoren versetzt, die über Temperaturunterschiede innerhalb der Rohre Energy Harvesting betreiben und somit kontinuierlich Daten übermitteln können, ohne einen physischen Zugang zu bedingen. Dies ermöglicht, nach der anfänglichen Implementierung, eine selbstständige und nachhaltige Netzüberwachung und somit eine

Optimierung des Asset Managements (Maurer und Ebi o. J.).

Auch anhand von piezoelektrischen Komponenten kann Energy Harvesting betrieben werden, um mittels kinetischer Energie Sensoren zu betreiben. Beispielanwendungen findet man in der Verkehrsinfrastruktur, wo es Versuche gibt, Brücken- oder Tunnelsensoren durch die vom Verkehr verursachten Vibrationen anzutreiben (Gkoumas et al. 2012).

#2 Cyberrisiken

Durch die vermehrten Verknüpfungen zum Internet bestehen im IoT neue Angriffspunkte. Die Datenübertragung und die Hauptplattform der IoT-Komponenten sind aufgrund dessen für Cyberangriffe besonders anfällig. Wegen der zentralisierten Datensicherung sind von einem Angriff alle persönlichen und betrieblichen Daten sowie die Kommunikation der IoT-Komponenten gefährdet (Koo et al. 2015). Häufige Angriffsmuster sind DDoS Angriffe, Hacken, Datendiebstahl und Fernsteuerung (Dogo et al. 2019).

Vulnerabilität der Sensoren

Aufgrund der geringen Ressourcen, über die die Sensoren verfügen, ist die Implementierung von rechenintensiven Sicherheits- und Schutzmaßnahmen erschwert, was insbesondere zu einem Datendiebstahl führen kann. Zudem lassen sich die Komponentenchips leicht klonieren, wodurch weitere Cyberangriffe ermöglicht werden (Lee 2020). Aufgrund der übergeordneten Vernetzung von Sensoren des IoT sind Botnets eine weitere Gefahr: Indem Sensoren von Angreifern aufgrund ihrer geringen Rechenkraft und Schutzmaßnahmen übernommen werden, können sie als Teil eines neuen Netzes für komplexere Angriffe weitergenutzt werden (Ramani und Iyengar 2017).

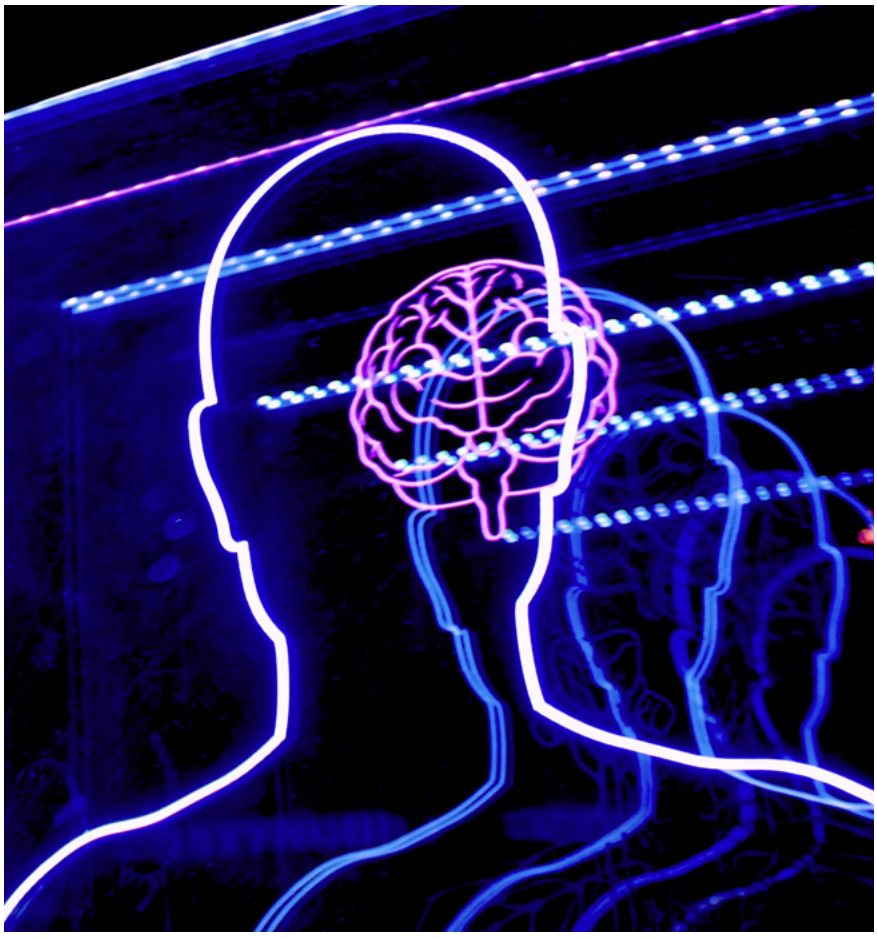
Insbesondere Smart Meter sind aufgrund der niedrigen Komplexität des Gerätes sowie der physischen Nähe zu möglichen Angreifern besonders gefährdet. Über direkt oder indirekt eingespeiste Firmware, der Beeinträchtigung der Hardware oder Eingriffe in die Kommunikation des Gerätes können Cyberangriffe ausgeführt werden (Sun et al. 2021). Aufgrund der Verbindung des Smart Meters zum übergeordneten Netzwerk können sich Angreifer somit einen Zugang zu weiteren Teilbereichen der kritischen Infrastruktur verschaffen.

Risiken der Sensoren (-netzwerke) betreffen vor allem die Modifizierung der Daten oder die Verhinderung des Datenflusses. Zum einen birgt die Steuerung von Anlagenkomponenten aus der Ferne durch das Einwirken auf die Sensoren oder auf angeschlossene Controller Risiken. Zum anderen können selbst komplett automatisierte (und theoretisch isolierte) Steuerungsprozesse, z. B. durch die Einschleusung falscher Daten, noch immer indirekt beeinflusst werden und somit schlussendlich die komplette Infrastruktur beeinträchtigen (Tuptuk et al. 2021).

Fehlende Interoperabilität

Aufgrund der Vielfältigkeit von Technologien, die in einem IoT-System einbezogen werden, können Schwierigkeiten bei der Interoperabilität und Standardisierung entstehen, was zu Sicherheitslücken führen kann (Dogo et al. 2019). Zudem erschweren die heterogenen Komponenten und unterschiedlichen Standards des IoT die Schaffung von übergreifenden Cybersicherheitsrahmen und -maßnahmen (Reeves und Maple 2018, Lu und Xu 2019). Deswegen ist es für die weitere Entwicklung der Wasserinfrastruktur unentbehrlich, dass Sicherheitsmaßnahmen oder deren Voraussetzungen, wie geeignete Interoperabilitätsrahmen, direkt von Herstellern in den Komponenten eingebaut werden (Wang et al. 2017). Der Security by Design Ansatz beschreibt die Beachtung von Cybersicherheitsmaßnahmen und -standards schon beim Entwurf der Komponenten und kann, zusätzlich zu einer Verbesserung der Cyberisicherheit und einhergehenden Verringerung der Kosten von Schutzmaßnahmen, Endnutzer:innen die Kontrolle der Komponenten erleichtern, sowie die Leistung der Komponenten verbessern (Javed et al. 2017).

Künstliche Intelligenz



KI für das Wassermanagement

Der Weltmarkt für KI, der derzeit auf zwei Billionen US-Dollar geschätzt wird, wird Prognosen zufolge bis 2030 auf 16 Billionen US-Dollar anwachsen. Es wird erwartet, dass KI die nächste Ära der technologischen und wirtschaftlichen Entwicklung vorantreiben wird, ähnlich stark wie die industrielle Revolution und die Einführung intelligenter Geräte (Mehmood et al. 2020). Der Wassersektor bildet hier keine Ausnahme. In den letzten zehn Jahren hat das generierte Datenvolumen exponentiell zugenommen. Nach Angaben von Forbes werden täglich 2,5 Quintillionen Byte unstrukturierter Daten erzeugt. Parallel dazu hat der wachsende Zugang zu Rechenleistung die Möglichkeit geschaffen, Daten zu analysieren, das Verhalten komplexer Systeme zu verstehen und die Funktionsweise natürlicher und städtischer Systeme zu simulieren. Die KI-gestützten Innovationen und Maßnahmen im Wassersektor werden im Jahr 2030 einen positiven Einfluss von schätzungsweise 200 Milliarden US-Dollar haben, was 0,04 % bis 0,2 % des globalen BIP entspricht (PwC 2019). Dieser mag im Vergleich zum Einfluss von KI auf andere Branchen gering erscheinen, aber die dadurch geschaffenen Effekte werden eine entscheidende Rolle bei der Erhaltung des Umweltschutzes und der Abschwächung der Auswirkungen des Klimawandels spielen.

In einer kürzlich durchgeführten Foresight-Studie der UNU wurden fünf Schlüsselanwendungen identifiziert, bei denen der Einsatz von KI in der städtischen Wasserwirtschaft in den nächsten Jahrzehnten zunehmen wird (Mehmood et al. 2020).

Vorausschauende Wartung der Wasserinfrastruktur

KI für die vorausschauende Instandhaltung ist bereits eine wichtige Säule der Industrie 4.0 (Lasi et al. 2014) und wird nun langsam auch von Wasserversorgern angenommen: 2016 nutzten weniger als 20 % der Betreiber in den USA KI-Lösungen zur Optimierung von Wartung und Betrieb (Mercer 2016). KI ermöglicht einen Wechsel von vorbeugenden Wartungssystemen mit planmäßigen Inspektionen der Wasserinfrastruktur hin zu einer vorausschauenden Wartung. Dabei werden intelligente sensorisch-physikalische Systeme zur Überwachung der Wasserinfrastruktur sowie zur Planung von Inspektion, Wartung und Infrastruktursanierung auf der Grundlage des Anlagenzustands eingesetzt. Die meisten Städte sind heutzutage mit dem Problem einer alternden Infrastruktur konfrontiert, die umfassend modernisiert werden muss. Es wird daher erwartet, dass die Sicherung der Servicequalität unter leistbaren Wassertarifen die Einführung von Lösungen für die vorausschauende Wartung fördern wird. Die Stadt Seoul beispielsweise setzt bereits KI ein, um Defekte im Netz automatisch zu erkennen. Das System identifiziert automatisch strukturelle Probleme in der Kanalisation anhand von TV-Inspektions-Bildern und soll langfristig die manuelle Kanalinspektion ersetzen (SmartCitiesWorld 2021). In Berlin setzen die Berliner Wasserbetriebe bereits KI ein, um den baulichen Zustand der 10 000 km langen Kanalrohre auf der Grundlage ihrer Hauptmerkmale und Umwelteinflüsse, wie die Verkehrsbelastung, zu simulieren. Diese neuen Informationen werden genutzt, um Inspektionen zu priorisieren und die Effizienz von Sanierungsprogrammen zu erhöhen (SEMAplus). Kürzlich wurde eine neue Nutzergemeinschaft (SEMAplus-Community) gegründet, um den Austausch zwischen den Betreibern zu erleichtern und die Einführung datengestützter Asset-Management-Tools zu fördern (KWB 2022). Die Erfahrungen werden derzeit auf Trinkwasseranlagen übertragen, wobei KI eingesetzt wird, um den Betreibern bei der Umstellung von der zeitbasierten Wartung einzelner Brunnen auf eine zustandsorientierte Wartung mit Blick auf alle verfügbaren Brunnen zu unterstützen (digital-water.city 2022).

Vorhersage von Wasserbedarf und -verbrauch

KI-gestützte Wassermanagementsysteme werden es Betreibern ermöglichen, Wasserverbrauch und -bedarf zu überwachen und die Leistung des Wassersystems in Echtzeit zu analysieren (Water Intelligence o. J.). Die Verarbeitung von Daten zu Wasserverbrauch und -nachfrage mit Deep-Learning-Technologie hat eine neue Generation von Wassermanagementsystemen ermöglicht, die kurzfristige (tägliche) und langfristige (jährliche) Prognosen erstellen können. Kurzfristige Prognosen werden

Um die Vielfalt der Anwendungen im Wasser- und Umweltsektor zu verstehen

Mehmood, H. et al. (2020) Strategic Foresight to Applications of Artificial Intelligence to Achieve Water-related Sustainable Development Goals. UNU-INWEH Report Series, Issue 09. UNU-INWEH, Hamilton, Canada.

für die effiziente Verwaltung der Wasserinfrastruktur verwendet (Guo et al. 2018). Langfristige Prognosen werden für die Planung und den Ausbau von Wassernetzen verwendet (Pacchin et al. 2019). Thames Water, das größte Wasser- und Abwasserunternehmen des Vereinigten Königreichs, nutzt beispielsweise KI zur Vorhersage des Bevölkerungswachstums, der Anzahl der Haushalte, die sich in Wasserressourcenzonen befinden, und des daraus resultierenden Wasserverbrauchs. Diese Vorhersagen werden verwendet, um die Auswirkungen auf den Pro-Kopf-Wasserverbrauch und die Gesamtnachfrage für politische Optionen (Messprogramm, innovative Tarife) zu bewerten.

Überwachung der Wasserqualität

Die Aufrechterhaltung einer guten Wasserqualität ist eine der größten Herausforderungen, der sich die Gesellschaft im 21. Jahrhundert stellen muss (UNESCO 2021). Das Zusammenspiel von IoT- und KI-Technologien bietet unzählige Anwendungsmöglichkeiten: KI kann zur Vorhersage der Wasserqualität in Wasser- und Kanalisationsnetzen in Echtzeit (DHI o. J.), zur Überwachung der Wasserqualität durch Mustererkennung zur schnellen Erkennung der Bakterienkonzentration (FLUIDION o. J.) und zur Fernerkundung der Wasserqualität (aqua3S o. J.) eingesetzt werden.
Es wird auch erwartet, dass kostengünstige tragbare Geräte zur Verfügung stehen werden, die an Smartphones angeschlossen werden können und mit denen KI Wasserproben automatisch und ohne die Hilfe eines Labors analysieren kann (Ingles et al. 2021, Shin et al. 2021). Solche kostengünstigen Sensoren würden Bürger:innen, Haushalten oder Betreibern zur Verfügung stehen, um die Wasserqualität in Echtzeit zu überwachen und das Potenzial der Citizen Science freizusetzen. So haben Forscher vor Kurzem eine kostengünstige Lab-on-a-Smartphone (LOS)-Plattform für die schnelle Vor-Ort-Überwachung von fäkalen Indikatorbakterien entwickelt. Mit einem Smartphone werden digitale Bilder von Zielwasserproben aufgenommen und deren zeitabhängige RGB-Werte analysiert (Thio et al. 2022).

Überwachung und Vorhersage wasserbedingter Katastrophen

Von 2001 bis 2018 ereigneten sich weltweit über 5 000 wasserbedingte Katastrophen, die knapp 80 % aller Naturkatastrophen ausmachten. Überschwemmungen, Stürme, Erdrutsche und Dürren verursachten weltweit über 300 000 Todesopfer und massive wirtschaftliche Schäden und hatten in der jüngeren Geschichte erhebliche wirtschaftliche Auswirkungen (Lee et al. 2020).
KI hat das Potenzial, eine wichtige Rolle bei der beschleunigten Einführung von Instrumenten für die Prävention, das Management und die Bewertung von wasserbezogenen Katastrophen zu spielen. So nutzt beispielsweise Google über sein Programm Google Public Alerts in Indien KI zur Ausgabe von Flutwarnungen. Das Warnsystem nutzt Daten aus historischen Hochwasserereignissen, Messungen des Flusspegels und der Morphologie, um Algorithmen des maschinellen Lernens zu trainieren. Diese sind in der Lage, Hochwasserereignisse und deren Schweregrad vorherzusagen (Vincent 2020). In Japan versuchen Forscher:innen der Universität Tokio das landesweite Hochwasservorhersagesystem zu verbessern, indem sie viel früher vor den Auswirkungen von Taifunen warnen (Ma et al. 2021).

Schaffung von digitalen Zwillingen städtischer Wasserinfrastrukturen

Unbedingt lesen: für das Potenzial von KI für Cybersicherheitsanwendungen

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021) Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2 (3): 1-18.

In den letzten Jahren hat sich das Konzept des digitalen Zwillings als eine Möglichkeit herauskristallisiert, Modellierungssysteme mit den Echtzeit-Datenströmen zu verbinden, die den Stand der Infrastrukturen überwachen. Eine Schlüsselkomponente digitaler Zwillinge, die sie auch von traditionellen Modellierungsansätzen unterscheidet, ist ihre Fähigkeit, Online-Daten zu nutzen, um ein kontinuierlich aktualisiertes Bild der physischen Infrastruktur zu liefern (Grieves und Vickers 2017). Während ein validiertes Modell eine Momentaufnahme des Verhaltens eines Systems auf einer bestimmten Zeitskala liefern würde, erweitert der digitale Zwilling die Verwendung dieses Modells auf Zeitskalen, in denen sich das Objekt und sein Verhalten erheblich ändern (Caradot et al. 2022). Künstliche Intelligenz gilt als eine der zugrundeliegenden Kerntechnologien für den digitalen Zwilling der Zukunft. KI könnte als das Gehirn des Zwillings angesehen werden, das notwendig ist, um die enor-

men Datenmengen zu verarbeiten, die das System erzeugt, und um sein Verhalten selbst zu optimieren. Der Einsatz von KI in digitalen Zwillingen steckt noch in den Kinderschuhen, doch wird erwartet, dass er mit der Weiterentwicklung von 5G und anderen hochmodernen Kommunikationstechnologien eine immer größere Rolle spielen wird (Lv und Xie 2021).
Erste vielversprechende Beispiele für digitale Zwillinge werden für die Verwaltung von Wasserinfrastrukturen eingesetzt. In den USA wurde ein digitaler Zwilling entwickelt, indem Daten der Advanced Metering Infrastructure (AMI) mit einem hydraulischen Modell gekoppelt wurden, um neue Verbrauchsmuster und ihre Auswirkungen auf das Funktionieren von Wassersystemen im Zusammenhang mit der Covid-19-Pandemie zu untersuchen und zu visualisieren (Pesantez et al. 2022). In Spanien wurde für die Stadt Valencia ein digitaler Zwilling entwickelt, der das hydraulische Modell des Wassernetzes mit einer Datenplattform verbindet, die alle von der Advanced Metering Infrastructure (AMI), den Computerized Maintenance Management Systems (CMMS) und den Feldsensoren des SCADA-Systems gelieferten Informationen sammelt. Der digitale Zwilling wird jede Minute mit SCADA-Daten aktualisiert, um den Bedarf, den Druck, die Füllstände und den Status aller Elemente im System anzupassen (Conejos-Fuertes et al. 2020).
Über die optimierte Steuerung unserer physischen Systeme hinaus eröffnet der digitale Zwilling neue Horizonte für die Einbindung von Akteuren mit immersiven und spielerischen Erfahrungen durch Serious Gaming oder virtuelle Realität (Savić 2021). Wasserbetreiber beginnen damit, digitale Zwillinge ihrer Anlagen und Einrichtungen mithilfe von 3D-Laserscans zu erstellen, um die Fernüberwachung und -steuerung zu ermöglichen und immersive Schulungsprogramme zu entwickeln (Sacyr 2022). Auf städtischer Ebene werden digitale Zwillinge zur Erleichterung des Wissensaustauschs zwischen Interessengruppen und Bürger:innen eingesetzt, z. B. in der deutschen Stadt Herrenberg zur Visualisierung künftiger städtischer Entwürfe, Szenarien oder der Auswirkungen von Risiken (Dembski et al. 2020; Magloff 2022).

KI für Cybersicherheit

Wenn KI ein großes Potenzial für die Verbesserung der Nachhaltigkeit der städtischen Wasserwirtschaft aufweist, wird sie voraussichtlich auch eine Schlüsselrolle für die Cybersicherheit im Wassersektor spielen. KI-Methoden, die auf der Modellierung von Sicherheitsintelligenz beruhen, können zur Lösung verschiedener Cybersicherheitsprobleme und -aufgaben eingesetzt werden, z. B. zur automatischen Identifizierung bösartiger Aktivitäten, zur Erkennung von Phishing und Malware, zur Vorhersage von Cyberangriffen, zur Erkennung von Betrug, zur Verwaltung von Zugangskontrollen, zur Erkennung von Anomalien oder Eindringlingen usw. KI-basierte Modellierung kann den Cybersecurity-Computing-Prozess handlungsfähiger und die Entscheidungsfindung im Vergleich zu herkömmlichen Systemen intelligenter machen (Sarker 2021). Die Aussichten für KI in Cybersicherheitsanwendungen sind groß und aktuelle Implementierungen zeigen bereits ihr Potenzial. Zunächst wird erwartet, dass KI die Angriffsprävention verbessern wird, indem sie unsere Fähigkeit erhöht, Bedrohungen zu erkennen und zu verfolgen (Tufan et al. 2021). Dann wird KI die Robustheit unserer Systeme verbessern, insbesondere die Fähigkeit eines Systems, sich auch dann wie erwartet zu verhalten, wenn es fehlerhafte Eingaben verarbeitet, dank selbsttestender und selbstheilender Software (Taddeo 2019; King 2019). Schließlich wird die KI die automatische Reaktion unserer Systeme verbessern, d. h. die Fähigkeit einen Angriff selbstständig abzuwehren, künftige Strategien zu verfeinern und möglicherweise mit jeder Iteration aggressivere Gegenmaßnahmen einzuleiten. KI-Systeme, die die Reaktion auf Angriffe unterstützen und Honeypots für Angreifer generieren, sind bereits auf dem Markt erhältlich (ACALVIO 2022).

Innerhalb des großen Bereichs der KI können Methoden des maschinellen Lernens und des Deep Learning für verschiedene Zwecke eingesetzt werden, z. B. zur Erkennung von Netzwerkeinbrüchen, zur Erkennung und Klassifizierung von Malware-Verkehr, Backdoor-Angriffen usw. (Jo et al. 2015; Almiani et al. 2020; Mitchell et al. 2014). Solche Modelle können aus den Trainingsdaten lernen und sich in den ungesehenen Testfällen entsprechend verhalten. Klassifizierungslernen ist ebenfalls eine beliebte Technik, die mit Tools wie Entscheidungsbäumen (Sarker 2020) zur Bewertung von Netzwerkeinbrüchen verwendet werden kann.

Die Verarbeitung natürlicher Sprache (Natural Language Processing, NLP) gilt als wichtiger Zweig der KI, der es Computern ermöglichen kann, menschliche Sprache zu verstehen, zu interpretieren und schließlich zu bestimmen, welche Teile in einem intelligenten System wichtig sind. Eine Schlüsselanwendung von NLP ist die semantische Analyse, die das Verständnis des Kontexts und der

Wahrnehmung von Wörtern und der Struktur von Sätzen umfasst. So kann beispielsweise bei der Klassifizierung von Phishing die latente semantische Analyse zusammen mit der Extraktion von Schlüsselwörtern verwendet werden (L'Huillier 2010). Die am weitesten verbreiteten Techniken in der NLP sind die Entitätserkennung (NER), die Wortsinn-Disambiguierung, die Erzeugung natürlicher Sprache usw. Ein auf NER basierendes automatisiertes System (Georgescu 2019) kann beispielsweise zur Diagnose von Cybersicherheitssituationen in IoT-Netzwerken verwendet werden.

Zu guter Letzt ist eine hilfreiche Anwendung von KI die Immunität. Wenn eine KI wie das Immunsystem des menschlichen Körpers trainiert werden kann, wird sie in der Lage sein, alle Bedrohungen viel schneller und effektiver zu lokalisieren und zu neutralisieren. Weiße Blutkörperchen und Antikörper neutralisieren Bedrohungen, die nicht den bekannten Mustern entsprechen, ohne das gesamte System auszuschalten. Das System kann aus früheren Erfahrungen lernen und stärker werden, ähnlich wie ein Organismus, der einer Infektion ausgesetzt war (Chan 2019).

Die Entwicklung von KI-Lösungen und das Aufkommen von Low-Code/ No-Code-Plattformen

Da sich die technologische Landschaft schnell weiterentwickelt, wächst die Nachfrage nach KI-Lösungen für Wasserinfrastrukturen schnell. Die Entwicklung von Software-Tools für den Einsatz von KI-Anwendungen umfasst große Mengen an Code und erfordert die Einbeziehung von Expert:innen mit speziellen Fähigkeiten und Talenten in den Bereichen Programmierung, maschinelles Lernen, Interoperabilität und Informatik. Um dem Bedarf an schneller und effizienter Softwareentwicklung gerecht zu werden, sind No-Code-Plattformen – und ihre Low-Code-Verwandten, die minimale Programmierkenntnisse erfordern – derzeit auf dem Vormarsch. Diese Plattformen ermöglichen es Entwickler:innen, vorcodierte „Blöcke“ per Drag-and-Drop zu erstellen. Sie stellen einen wichtigen Schritt auf dem Weg zu dem ehrgeizigen Ziel dar, die Codierung bei der Entwicklung von Softwareanwendungen zu automatisieren (Sanchis et al. 2020). Das Wertversprechen der Low-Code-Technologie besteht darin, dass sie Betreibern die Agilität verleiht, sich an die sich schnell verändernde Branchenrealität anzupassen, indem sie die Markteinführungszeit neuer Anwendungen beschleunigt (visio.ai o. J.). Laut einer Gartner-Prognose werden über 50 % der mittleren bis großen Unternehmen bis 2023 Low-Code/ No-Code-Plattformen als Teil ihrer IT-Gesamtstrategie einsetzen (Gartner 2021). Die meisten Software-as-a-Service (SaaS)-Anbieter stellen bereits Funktionen zur Verfügung, die Low-Code-Entwicklungstechnologien beinhalten. Da SaaS immer beliebter wird, wird erwartet, dass der Low-Code-Markt ein entsprechendes Wachstum bei Low-Code-Anwendungsplattformen und Tools zur Prozessautomatisierung verzeichnen wird.

2019 hat Anglian Water begonnen, die Low-Code-Plattform von Appian zu nutzen, um die Entwicklung neuer digitaler Geschäftsanwendungen zu beschleunigen. Ihre Lösung mit der Bezeichnung Totex Delivery Workflow (TDW) bietet den Mitarbeiter:innen eine einheitliche und intuitive Sicht auf alle relevanten Versorgungsdaten, unabhängig davon, wo sich die Daten in den Altsystemen des Betreibers befinden. Sie ermöglicht die schnelle Entwicklung von maßgeschneiderten Datenanalyselösungen zur Digitalisierung und Automatisierung von Geschäftsprozessen (Appian 2019). Suez hat auch damit begonnen, kostengünstige Plattformen zur Optimierung der Abfallentsorgungsdienste zu nutzen, mit dem Ziel, Anwendungen innerhalb von Wochen statt Monaten auf den Markt zu bringen (Mendix 2019). Eine Suez-Einheit im Vereinigten Königreich vertraute auf Mendix, ein führendes Siemens-Unternehmen im Bereich kostengünstiger Plattformen, um ein maßgeschneidertes Tool zur Preisgestaltung für Kunden zu entwickeln, das Self-Service-Angebote für die Abfallentsorgung, einschließlich Preissimulation, liefert.

#2 Cyberrisiken

Die neuen Risiken, die durch die Einführung von KI-Lösungen entstehen, stehen in direktem Zusammenhang mit den Schwachstellen und Grenzen der KI.

Frühere Generationen von Cyberangriffen zielten hauptsächlich darauf ab, Daten zu stehlen (Extraktion) und Systeme zu zerstören (Störung). Neue Formen von Angriffen zielen auch auf KI-Systeme ab und versuchen, die Kontrolle über das Zielsystem zu erlangen und dessen Verhalten zu ändern. Um die Kontrolle zu erlangen, sind drei Arten von Angriffen besonders relevant: Datenvergiftung, Beeinflussung von Kategorisierungsmodel-

len und Backdoors (Biggio 2018).

Angreifer können beispielsweise **fehlerhafte Daten in legitime Daten einfügen**, die zum Trainieren des Systems verwendet werden, um dessen Verhalten zu ändern. Es wäre möglich, die Ergebnisse der KI leicht zu verändern und das datengesteuerte Entscheidungsverfahren zu beeinflussen. Diese Art von Angriff könnte z. B. die Dosierung von Chemikalien für die Trinkwasseraufbereitung oder andere kritische Vorgänge beeinflussen. Experimente in der Gesundheitsbranche haben gezeigt, dass Datenvergiftung zu erheblichen Änderungen der von Algorithmen des maschinellen Lernens vorgeschlagenen Medikamentendosierungen führen kann und potenziell zu schädlichen Situationen führt (Jagielski et al. 2018).

Ein zweites Problem ist, **dass Cyberangriffe auf KI-Algorithmen aufgrund der Eigenschaft der KI sehr schwer zu erkennen sind**. Die adaptive Eigenschaft von KI-Systemen macht es schwierig, ihre internen Prozesse zu erklären und ihr Verhalten zurückzuentwickeln (Taddeo 2019). Insbesondere kann es äußerst schwierig sein, festzustellen, ob das System aufgrund eines Angriffs ein „falsches“ Verhalten zeigt, da der Angriff zu minimalen Abweichungen vom erwarteten Verhalten führen kann. Forscher:innen in den USA haben gezeigt, wie die Manipulation von CCTV-Bildern (z. B. durch die Erzeugung von fiktivem Zubehör für die beobachtete Person) KI-Bilderkennungssysteme austricksen und zu einer Fehlklassifizierung führen kann. Angreifer könnten sich mit einer solchen Technik Zugang zu geschützten Einrichtungen verschaffen, ohne dass ein Sicherheitsverstoß gemeldet wird (Sharif et al. 2016).

Aufgrund der mangelnden Transparenz und der Lernfähigkeit von KI-Systemen lässt sich nur schwer beurteilen, ob sich ein und dasselbe System in einem bestimmten Kontext weiterhin wie erwartet verhalten wird. Aufzeichnungen über das frühere Verhalten von KI-Systemen sagen weder etwas über die Robustheit der Systeme gegenüber künftigen Angriffen aus, noch sind sie ein Hinweis darauf, dass das System nicht durch einen ruhenden Angriff (z. B. durch ein Backdoor) oder einen noch nicht entdeckten Angriff beschädigt wurde. Dies beeinträchtigt die Bewertung der Vertrauenswürdigkeit. Solange die Bewertung der Vertrauenswürdigkeit problematisch bleibt, wird das Vertrauen in KI-Anwendungen für die Cybersicherheit ungerechtfertigt bleiben (Chan 2019).

Cloud-Migration und IT/OT-Integration

#1 Trends

Cloud Computing: neue Vorteile für den Wassersektor

In den letzten drei Jahren ist die Menge der Daten, die Betreiber täglich sammeln, erheblich gestiegen und Cloud-Lösungen gelten als Schlüsseltechnologie für die Bewältigung des Wachstums von IoT-Geräten. Die Cloud-Technologie bietet Vielseitigkeit mit skalierbaren Lösungen, außergewöhnlicher Rechenleistung, praktisch unbegrenztem Datenzugriff und potenziellen Kosteneinsparungen, die Betreibern bei ihren Tätigkeiten helfen (Buyya et al. 2018).

Definitionsgemäß ist die Skalierbarkeit der Cloud-Plattform ihre Hauptstärke im Vergleich zum traditionellen Hosting. Für die Anforderung zusätzlicher Kapazitäten sind keine komplexen Prozesse oder sogar vollständige Beschaffungszyklen mehr erforderlich, da Kapazitätserweiterungen von der gehosteten Anwendung gesteuert werden können. Die Technologie hat das Potenzial, die Unternehmensleistung über die Kostenreduzierung hinaus in vielerlei Hinsicht zu verbessern. So können Betreiber beispielsweise experimentieren und ihre Lösungen verbessern, was Flexibilität und Agilität bei minimalen Investitionen ermöglicht (Microsoft 2016, Thomas 2020).

Für einen Überblick über Cybersicherheitsprobleme und Lösungen für industrielle Kontrollsysteme (ICS)

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020) Cybersecurity for industrial control systems: A survey. computers & security, 89, 101677.

Die Einführung von Cloud Computing durch Betreiber

Laut einer aktuellen Accenture-Studie investierte der Versorgungssektor 2019 weltweit mehr als vier Milliarden US-Dollar in Public-Cloud-Lösungen (Thomas 2020.). Ab 2021 werden rund 50 % aller Unternehmensdaten in der Cloud gespeichert sein. Im Jahr 2015 lag dieser Anteil erst bei 30 % und ist weiter gestiegen, da Unternehmen ihre Ressourcen zunehmend in Cloud-Umgebungen verlagern (Statista). Eine kürzlich durchgeführte Umfrage unter mehr als 150 Führungskräften von Betreibern (darunter 35 % aus dem Wasser- und Abwassersektor) aus der ganzen Welt ergab, dass sich das Tempo der Einführung und der Umfang der Anwendungen, die in die Cloud verlagert werden, deutlich beschleunigen. Im Jahr 2019 nutzt eine große Mehrheit (71 %) der Betreiber bereits Cloud-Software, im Jahr 2016 waren es nur 45 % (Oracle 2019). Doch auch wenn Fortschritte erzielt wurden, nennen 85 % der Befragten immer noch die Sicherheit als wichtigstes Anliegen und stellen fest, dass die Akzeptanz durch die Behörden ein Hindernis für die Cloud-Einführung bleibt. Die Einführung der Cloud erfolgt viel schneller in Bereichen wie Verkauf, Vertrieb oder Kundendienst als bei sensiblen Vorgängen wie SCADA-Systemen, die größere Sicherheitsbedenken aufwerfen. Diese Aussage wird durch eine Untersuchung über die Nutzung von Cloud-Computing-Diensten speziell für den Sektor der kritischen Infrastrukturen gestützt, die ergab, dass nur 22,5 % Cloud-Dienste nutzen (Adelmeyer 2018). Kritische Infrastrukturen sind traditionell zurückhaltend bei der Einführung von Cloud-Lösungen, da IT-Systeme ein wesentliches Element für die Erbringung ihrer Dienstleistungen sind (BSI 2017; 2021). Die Einführung von Cloud-Lösungen stößt an verschiedenen Fronten auf Widerstand, z. B. in Bezug auf Cybersicherheit, Compliance, Kosten und Latenzzeiten (Chung et al. 2014; Zhang et al. 2022; SmartEnergy 2020). Betreiber hosten häufig ihre eigene IT-Infrastruktur oder teilen sich Ressourcen mit Organisationen mit ähnlichen Anforderungen.

Die Übernahme von Cloud-Lösungen durch kritische Infrastrukturen erfolgt relativ langsam, ist aber eindeutig auf dem Vormarsch. UP KRITIS – eine öffentlich-private Zusammenarbeit zwischen Betreibern kritischer Infrastrukturen, ihren Verbänden und den zuständigen staatlichen Stellen – hat kürzlich Empfehlungen für die Nutzung von Cloud-Diensten in kritischen Infrastrukturen veröffentlicht (UP-KRITIS 2020). Dieser Trend wird auch durch die zunehmende Einführung von IoT-, Smart-Metering- und Smart-City-Lösungen unterstützt, die in den nächsten zehn Jahren den größten Anteil an der Migration zum Cloud Computing haben dürften (Oracle 2019). Während Betreiber ihre Digitalisierung vorantreiben, wird die Menge an Daten, die sie verwalten, analysieren und in ihren Entscheidungsprozessen berücksichtigen müssen, die Flexibilität erfordern, die eine Cloud bieten kann.

Die Gaia-X-Plattform ist ein europäisches Projekt, das genau diesen Trend begleiten und eine standardisierte Cloud-Netzinfrastruktur auf europäischer Ebene schaffen soll (Gaia-X 2021). Die Architektur von Gaia-X basiert auf dem Prinzip der Dezentralisierung mit der

Zusammenschaltung einer Vielzahl von einzelnen Clouds, die mit gemeinsamen Standards für die Interoperabilität verbunden sind. Gaia-X führt bestehende Cloud-Anbieter und ihre Dienste in einer neuen modularen Umgebung zusammen, die auf Open-Source-Prinzipien beruht. Die Initiative zielt auch darauf ab, ein Ökosystem zu schaffen, das die digitale Souveränität der Nutzer:innen von Cloud-Diensten stärkt und den europäischen Cloud-Anbietern hilft, ihre Wettbewerbsfähigkeit zu verbessern. Die Betreiber würden von einem integrierten Rahmen mit strengen Anforderungen an die Informationssicherheit, Rechtssicherheit im Rahmen der europäischen Datenschutzgrundverordnung (DSGVO) und der Datenspeicherung in Europa profitieren.

Beispiele für Cloud-Migration im Wassersektor

Betreiber migrieren zunehmend IT-Dienste in Cloud-Umgebungen und Analyst:innen gehen davon aus, dass die Nutzung in den nächsten zehn Jahren stark zunehmen wird (Microsoft 2016; Schöller et al. 2013, Chalmers 2020). Eine kürzlich durchgeführte Umfrage im Vereinigten Königreich ergab, dass bereits 25 % der Wasserbetreiber ihre Einführung der Cloud-Technologie abgeschlossen haben (TCS 2016). Die folgenden Beispiele geben einen Einblick in die von führenden Betreibern eingeleiteten Migrationsprozesse.

Anglian Water, das größte Wasserunternehmen in England und Wales, hat ein Cloud-Hosting-Framework im Wert von 31 Millionen Pfund aufgelegt, das die Nutzung von IaaS- und PaaS-Diensten der Betreiber öffentlicher Cloud-Plattformen umfasst (tendersUK 2021).

Northumbrian Water Ltd. plante ebenfalls ein 4,6-Millionen-Pfund-Projekt zur Unterstützung der Migration von On-Premises-Infrastrukturen in die öffentliche Cloud. Das Unternehmen hat sich bereits für eine Multi-Cloud-Struktur entschieden, die Public-Cloud-Bereitstellungen auf AWS, Microsoft Azure und Oracle Cloud umfasst.

Auch Thames Water hat sich der digitalen Transformation verschrieben und beschlossen, seine Rechenzentren durch vier cloudbasierte Plattformen zu ersetzen: Microsoft Azure, Salesforce, SAP und AWS. Ein Hauptziel ist es, weniger abhängig von alten IT- und Systemintegratoren zu sein und den Weg für eine künftige Zusammenarbeit mit KMU und Lösungsanbietern zu ebnen (Reed 2021).

In ähnlicher Weise startete die Kommunalverwaltung von Singapur 2018 einen Fünfjahresplan, um die meisten ihrer IT-Systeme von der On-Premise-Infrastruktur in die kommerzielle Cloud zu migrieren. Seitdem hat sie mehr als 150 Systeme, die als „beschränkt“ und niedriger eingestuft wurden, in die kommerzielle Cloud verlagert. Für das Jahr 2020 waren Verträge im Wert von über 870 Millionen US-Dollar vorgesehen, um die Zahl der Systeme in der kommerziellen Cloud zu erhöhen. Auch der singapurische Wasserversorger PUB hat sich der Strategie angeschlossen und sein Programm für intelligente Wasserzähler in die Cloud migriert. Ziel ist es, den Wasserverbrauch der Haushalte drahtlos abzulesen und die Bürger:innen über ein Kundenportal mit Informationen über wassersparende Maßnahmen zu versorgen (GovTech Singapore 2020).

Die Konvergenz von IT- und OT-Technologien: eine neue Herausforderung für Wasserbetreiber

Die verschiedenen Komponenten moderner Wassersysteme werden im Allgemeinen über ein industrielles Kontrollsystem gesteuert, von denen das meistverbreitete die Supervisory Control and Data Acquisition Architecture oder das Prozessleitsystem (PLS) ist. SCADA-Systeme gehören zur Operational Technology, d. h. zu den Computersystemen, die zur Steuerung industrieller Prozesse verwendet werden, im Gegensatz zu den Verwaltungsprozessen (IT). Bei Standardanwendungen werden die von Sensoren vor Ort erfassten Daten an Steuerungskomponenten wie speicherprogrammierbare Steuerungen (SPS) übertragen, die in der Lage sind, die angeschlossenen Elemente der Anlagen (z. B. Pumpen, Ventile, Tanks) automatisch zu steuern. Die SPS übermitteln Daten an Master-Terminal-Units (MTU), die das Netz kontrollieren und regeln und von den Endnutzern über eine Mensch-Maschine-Schnittstelle (HMI) gesteuert werden. SCADA-Systeme werden in großem Umfang für die Prozesssteuerung, Datenerfassung, Systemüberwachung, Kommunikation mit industriellen Geräten und die Speicherung von Protokolldaten eingesetzt.

Für eine Analyse der Sicherheitsherausforderungen von OT-Netzen

Mansfield-Devine, S. (2019) The state of operational technology security. Network security 2019 (10): 9-13.

In der Vergangenheit und bis vor Kurzem wurde die Sicherheit von Wassersystemen bei den meisten Betreibern durch Isolierung erreicht, indem der Zugang zu den Steuerungskomponenten eingeschränkt wurde. OT-Systeme beruhten oft auf einer Art „Sicherheit durch Unklarheit“ (Rasekh et al. 2016). Außerdem sind die in OT-Systemen verwendeten Protokolle, Datenformate und Schnittstellen oft komplex und proprietär und unterscheiden sich stark von denen, die in IT-Systemen eingesetzt werden. Infolgedessen war es für einen Angreifer traditionell schwierig, ausreichende Kenntnisse und Fachwissen über diese Systeme zu erlangen, um einen erfolgreichen Angriff durchzuführen (Mansfield-Devine 2019).

Bei großen deutschen Betreibern sind IT- und OT-Systeme in der Regel vollständig physisch voneinander getrennt. Im Jahr 2014 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Bericht über den Stand der Cybersicherheit im Wassersektor, der auf einer Umfrage bei den größten Wasser- und Abwasserbetreibern des Landes basierte (BSI 2015). Alle Befragten gaben an, die IT- und OT-Netze logisch oder sogar physisch getrennt zu haben. Auch die Unterteilung von Systemen, Netzen und Infrastrukturen innerhalb der OT-Netze wurde häufig umgesetzt. In diesem Fall werden auf der Feldebene autonome Zonen gebildet, die auch bei einem Ausfall anderer Zonen unabhängig weiterarbeiten können. Während große Betreiber auf eine physische Trennung setzen, verfügen kleinere Betreiber in der Regel nicht über die notwendigen Ressourcen, um eine physische oder logische Trennung von IT und OT zu implementieren; sie sind auf ein gemeinsames Netzwerk angewiesen.

Große Betreiber setzen in der Regel auf ICS zur Überwachung von Anlagen und Netzen in einer zentralen Leitstelle. Allerdings steuerten 2014 nur wenige von ihnen die Anlagen auch von einer zentralen Stelle aus, da die Steuerung hauptsächlich über die Parametrierung der Steuerelemente in den Anlagen vor Ort erfolgte. Mit dem Aufkommen des IoT beginnen Betreiber, das IoT und die Analytik in das ICS einzubinden, um die Überwachung, aber auch die Steuerungskapazität des Betriebs zu verbessern. In Deutschland prognostiziert das BSI, dass sich die Rolle der zentralen Leitstellen von den traditionellen Überwachungsaufgaben zur vollständigen Steuerung der Anlagen verlagern wird (BSI 2015). Dieser Trend wurde von mehreren Interviewpartner:innen bestätigt.

Zusammengenommen wird dies als industrielles Internet of Things (IIoT) bezeichnet, das oft als Industrie 4.0 bezeichnet wird (Lu 2017), wobei das IoT auf industrielle Anwendungen angewendet wird. Die Konvergenz von IT- und OT-Technologien könnte metaphorisch als eine Konvergenz zwischen der digitalen und der physischen Welt beschrieben werden (Hahn 2016). Es wird erwartet, dass diese Konvergenz auch den Markt für OT-Lösungen verändern wird, indem die Zusammenarbeit zwischen IT- und OT-Anbietern intensiviert wird. Gartner prognostiziert, dass bis 2020 50 % der OT-Anbieter bedeutende Partnerschaften mit IT-Anbietern für gemeinsame IoT-Angebote eingegangen sein werden (Gartner 2021).

Insbesondere Infrastructure as a Service (IaaS) ist ein von Cloud-Anbietern angebotener Dienst, der in letzter Zeit stark an Bedeutung gewinnt. Die Industrie kann von solchen cloudbasierten Diensten profitieren, bei denen SCADA-Systeme und SPS-Steuerungen als Service unter Nutzung der von den Clouds bereitgestellten Infrastruktur implementiert werden können (Bhamare et al. 2019). Dadurch können erhebliche Kosten für Hardware und Infrastruktur eingespart werden. Die Anbindung von ICS-Komponenten an die Cloud und das Internet setzt sie jedoch einer wachsenden Zahl von Cyberangriffsszenarien aus.

Thames Water ist wieder ein interessantes Beispiel für diesen Wandel. Thames hat vor kurzem ein unternehmensweites Programm mit dem Namen „Intelligence Hub“ (iHub) eingeführt, um Big-Data-Analysen von Echtzeit-Betriebsdaten des PI-Systems aus mehr als 3 000 Anlagen und 140 000 km Wasser- und Abwassernetzen zu unterstützen. Daten von SCADA-Systemen und anderen Geräten werden an iHub weitergeleitet. Das System wurde von Thames entwickelt, um Betriebsdaten mit Unternehmensanwendungen wie SAP zu verknüpfen und so Kundendienste anzubieten. Das Projekt bezog sich zunächst nur auf Daten aus Trinkwassersystemen, wurde aber inzwischen auf den Abwasserbetrieb ausgeweitet. Durch die Kombination von IT und OT mithilfe des PI-Systems konnte Thames den Energieverbrauch bereits um fast zehn Prozent senken (OSIsoft 2017).

Für einen Return on Experience einer laufenden IT/OT-Integration

Maria Mülbaier (2021) Gute Perspektiven für Emscher und Lippe. 12.2021, gwf Wasser | Abwasser.

Sydney Water zeigt einen weiteren Treiber für die Beschleunigung der Konvergenz auf. Die Ausbreitung von nicht verwalteten digitalen Initiativen schaffte neue Angriffsvektoren und präsentierte eine zentrale Gefahr. Die Reaktion des Betreibers bestand darin, alle IT- und OT-Technologien in einer einzigen „Digitalen Gruppe“ zusammenzuführen, so dass es in der Lage ist, auf Bedrohungen und Schwachstellen in der gesamten digitalen Landschaft einheitlicher zu reagieren (Tagabe 2021).

Die Emschergenossenschaft und der Lippeverband (EGLV) haben einen im deutschen Kontext sehr innovativen Weg eingeschlagen, indem sie verschiedene kleinere Instanzen von Private Cloud Computing in ihrer Infrastruktur einsetzen. Die Cloud soll einen schnelleren Zugriff auf Daten und Dokumentationen gewährleisten, die Effizienz der Anlagen und Netze stärken und eine schnellere Reaktion, z. B. bei Starkregen oder Hochwasser, ermöglichen (NetApp 2018). Die Leitsysteme laufen auf einer virtualisierten Plattform in einem Rechenzentrum in Essen und verfügen über sichere Schnittstellen für den Fernzugriff. Der EGLV hat bereits abgeschätzt, dass er durch das zentralisierte und virtuelle System mindestens 20 % an Kosten einsparen kann, vor allem durch geringere Hardwarekosten, weniger Schulungen und geringere Lizenzkosten. Der einfachere Fernzugriff auf die Systeme und Anlagen hat sich auch bei den Einschränkungen der Corona-Pandemie bewährt, als die Techniker nicht vor Ort sein mussten, um Ausfälle zu beheben (Mülbaier 2021). Die Hauptvorteile für den EGLV sind eine erhöhte Flexibilität durch die Standardisierung von Steuerungssystemen (z. B. durch die Zusammenführung von mehr als 500 Anlagen, die mit ihren eigenen PLS unter einem Dach arbeiten), Skalierbarkeit und das Ebnen des Weges für die Entwicklung von vorausschauender Wartung und Big-Data-Anwendungen.

#2 Cyberrisiken

Das Hosting kritischer Infrastrukturdienste in der Cloud stellt hohe Anforderungen an die Ausfallsicherheit. Wie bereits erwähnt, sind Betreiber traditionell zurückhaltend, wenn es um die Einführung von Cloud-Lösungen geht, und die Einführung der Cloud stößt nach wie vor auf großen Widerstand, insbesondere was die Cybersicherheit betrifft.

Neue Sicherheitslücken

Eine besondere Herausforderung bei der Entwicklung von (allgemeinen IT-) Cloud-Anwendungen besteht darin, dass Cloud-Systeme besonders anfällig für Sicherheitsverletzungen sind (Paudel 2013). Dies liegt daran, dass solche Anwendungen in der Regel durch ihren verteilten Charakter mit einer erhöhten Anzahl von Datenübertragungs-/Speicherproblemen über das Internet zwischen dem Client und der Cloud-Anwendung gekennzeichnet sind.

Die Bewertung der verschiedenen Dimensionen der Cloud-Sicherheit ist eine umfangreiche Aufgabe und würde den Rahmen dieses Berichts sprengen. Zur Orientierung hat die Cloud Security Alliance (CSA) die zwölf größten Bedrohungen im Zusammenhang mit der Cloud sowie einen Leitfaden veröffentlicht, der Nutzer:innen dabei helfen soll, die geeignete Strategie zur Risikominderung zu ermitteln (CSA 2018). Younis et al. (2013) untersuchten die spezifischen Sicherheitsbedrohungen und Bedenken von Cloud-Computing-Anwendungen.

Generell können Sicherheitsfragen in vier Gruppen eingeteilt werden, die mit der Architektur der Cloud zusammenhängen: Datenebene, Anwendungsebene, Netzwerkebene und Host-Ebene (Saini et al. 2014). Die Sicherheit auf der Datenebene bezieht sich auf den Schutz von Daten, die sich in der Cloud befinden oder dorthin übertragen werden, um Datenverluste oder -lecks zu vermeiden. Datenschutzverletzungen sind ein kritisches Sicherheitsproblem, auf das man sich in der Cloud-Infrastruktur konzentrieren muss, da sich die Daten vom lokalen Rechner eines Kunden in eine vollständig gemeinsam genutzte Umgebung bewegen (Aich et al. 2015). Da in der Cloud große Datenmengen von verschiedenen Nutzern gespeichert werden, kann ein böswilliger Nutzer so auf die Cloud zugreifen, dass die gesamte Cloud-Umgebung angreifbar bleibt (Alghofaili et al. 2021). Der Angriff kann von einem internen Akteur mit Zugang zu den Daten oder von einem externen Akteur, der sich über die Cloud-Infrastruktur Zugang verschafft, verübt werden. Auf der Anwendungsebene beziehen sich die Risiken auf den Verlust der Kontrolle über die Anwendungen bei der Nutzung der Hardware- und Softwareressourcen. Die größten Bedrohungen sind Denial of Service (DoS), wenn ein Angriff darauf abzielt, die Anwendung abzuschalten und sie für die vorgesehenen Benutzer unzugänglich zu machen. Die Sicherheit auf Netzwerkebene bezieht sich auf den Schutz des Netzwerks bei der Verwendung einer virtuellen Firewall, einer

demilitarisierten Zone (DMZ) und von Daten im Transit (Alghofaili et al. 2021). Dazu gehört z. B. eine Firewall, die sich um die Kommunikation zwischen der virtuellen Infrastruktur und dem Rest des Netzwerks kümmert (Saini et al. 2014). Auf Host-Ebene sind die Hauptrisiken mit der Kompromittierung des virtuellen Servers, des Hypervisors und der virtuellen Maschine verbunden (Tank et al. 2019).

Datenintegrität, Datenschutz und Verfügbarkeit

Einer der kritischen Aspekte bei der konkurrierenden Sicherheit in der Cloud ist der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit der Daten. Die Daten werden in einer gemeinsamen Umgebung gespeichert und verschoben, die von verschiedenen Dienstanbietern verwaltet wird, und befinden sich wahrscheinlich in einem anderen Land, in dem andere Vorschriften gelten (Younis et al. 2013).

Der Schutz der Privatsphäre ist ein weiterer wichtiger Aspekt der Sicherheit beim Cloud Computing. Cloud Computing ist eine gemeinsam genutzte Umgebung, die eine gemeinsame Infrastruktur nutzt. Daher besteht das Risiko der Offenlegung von Daten oder des unbefugten Zugriffs. Die gemeinsame Nutzung von Cloud Computing-Ressourcen bei gleichzeitigem Schutz der Privatsphäre der Kund:innen ist eine große Herausforderung. Da die Daten auf verschiedenen Servern gespeichert sind, die sich an unterschiedlichen Orten befinden, wird die Datenverfügbarkeit aufgrund einiger Faktoren wie der Bandbreiteneffizienz zu einem großen Problem.

Neue Schwachstellen in OT-Netzen

Die Migration von ICS- und SCADA-Systemen in die Cloud kann zwar eine höhere Effizienz und Zuverlässigkeit bieten, doch sind die Systeme bei der Verlagerung in die Cloud möglicherweise neuen Bedrohungen und Schwachstellen ausgesetzt (Taormina et al. 2017). Im Zuge der Konvergenz von IT und OT sind herkömmliche Best Practices zur Schaffung von Luftlücken zwischen IT- und OT-Netzwerken schwer zu implementieren und unmöglich aufrechtzuerhalten. Die wachsende Angriffsfläche ermöglicht es über neuen Angriffsvektoren diese Netzwerke zu nutzen, um dadurch in die OT-Infrastruktur einzudringen (Rasekh 2016). ICS-Netzwerke verfügen über begrenzte Sicherheitskontrollen, die neue Möglichkeiten für den illegalen Zugang zu den Anlagen eröffnen könnten. Angriffe können auch dazu führen, dass die Verbindung zwischen entfernten Komponenten unterbrochen wird, was sich auf den Betrieb der Anlagen auswirkt und Kaskadeneffekte zwischen voneinander abhängigen Elementen eines komplexen Netzwerks auslöst. Durch die Entscheidung, kritische Informationen in der Cloud zu speichern, leiten Betreiber sensible Daten durch ein öffentliches Netzwerk, wodurch die Informationen zwangsläufig anfälliger für Hackerangriffe werden (Inductive Automation 2011).

Laut BSI (2019), welches kürzlich eine Liste mit den zehn kritischsten Bedrohungen für ICS veröffentlicht hat, sind ICS zunehmend denselben Cyber-Bedrohungen ausgesetzt wie herkömmliche IT-Systeme. Die Zahl der gemeldeten Angriffe auf ICS kritischer Infrastrukturen hat zugenommen. Die Angriffe können den Zugriff auf private Verbraucherdaten oder kritische betriebliche Informationen, die Beschädigung physischer Vermögenswerte (Pumpen, Rohre, Ventile, Anlagen), den Rückgang der Wasserversorgung und die Beeinträchtigung der Wasserqualität umfassen (Nikolopoulos et al. 2020).

Beispiele für Angriffe auf OT-Systeme sind zahlreich und sorgen regelmäßig für Schlagzeilen. Stuxnet wird weitgehend als der erste als Waffe benutzte Cyberangriff auf ein industrielles Steuerungssystem angesehen (Knapp et al. 2015). Stuxnet ist ein Computerwurm, der ursprünglich darauf abzielte, die iranischen Nuklearanlagen zu stören, der aber inzwischen mutiert ist und sich auf andere Industrie- und Energieerzeugungsanlagen ausgebreitet hat. Der ursprüngliche Angriff zielte auf die SPS, die zur Automatisierung der Zentrifugen in einer Urananreicherungsanlage verwendet wurden, und bewirkte, dass die Zentrifugen wild die Geschwindigkeit wechselten, bis sie zerstört wurden (Falliere et al. 2011). BlackEnergy ist ein weiteres Beispiel für einen äußerst raffinierten Angriff im Energiesektor: 2014 begann eine Gruppe von Angreifern, SCADA-bezogene Plugins im ICS eines Energiebetreibers in der Ukraine zu installieren, wodurch mehr als 200 000 Einwohner:innen für mehrere Stunden ohne Strom waren.

Ein größerer Angriff im Wassersektor ereignete sich im Jahr 2000 in Maroochy Shire, Australien. Ein verärgerter Bauunternehmer steuerte per Funk die Systeme einer Kläranlage und sorgte dafür, dass eine Million Liter Rohabwasser in die örtlichen Flüsse flossen (Slay 2007). Im Jahr 2016 verschaffte sich eine Hacktivistengruppe Zugang zu den SCADA-Systemen eines ungenannten US-Wasser-

versorgers. Es gelang ihnen, die Kontrolle über die SPS zu übernehmen, die den Wasserfluss und die zur Aufbereitung von Leitungswasser verwendeten Chemikalien regulierten (Leyden 2016).

Abgesehen von den Sicherheitsrisiken kann die Migration von ICS in die Cloud die Auslagerung von OT-Systemen an externe Dienstleister erforderlich machen (Apostu et al. 2014). Auch wenn Betreiber manchmal den IT-Betrieb an externe Cloud-Anbieter delegieren, wird OT im Allgemeinen als Kerngeschäft betrachtet und innerhalb der Organisation vertraulich behandelt (BSI 2015). Das OT-System würde von der Bandbreite und Latenz der Cloud-Dienste und Internetanbieter abhängig werden. Die Varianz der Latenz wird bei Cloud-basierten Systemen aufgrund der unvorhersehbaren Natur der Datenübertragung über das Internet noch verstärkt (Inductive Automation 2011). Die erhöhte und unvorhersehbare Latenz, die mit der Nutzung der Cloud verbunden ist, kann zu Problemen beim Echtzeitmanagement und zu Verzögerungen im Betrieb führen.

Umgestaltung der Infrastruktur und Dezentralisierung

Die neue technologische Landschaft, die in den vorangegangenen Abschnitten vorgestellt wurde, bietet den Betreibern neue Instrumente, Optionen und Szenarien zur Verbesserung der Planung und Verwaltung von Wassersystemen und zur Gestaltung der Entwicklung der städtischen Wasserinfrastruktur. Die vernetzte Infrastruktur, die derzeit von den meisten europäischen Städten zur Bewirtschaftung von Wasserversorgung, Abwasser und Regenwasser genutzt wird, wurde vor über 100 Jahren errichtet. Sie stützt sich traditionell auf investitionsintensive, unterirdische Rohrnetze, die Trinkwasser liefern und Regen- und Abwasser ableiten (Larsen et al. 2016).

Die Herausforderungen der traditionellen zentralisierten Systeme

Rückblickend betrachtet waren diese Infrastruktur und die mit ihrem Betrieb betrauten Organisationen sehr erfolgreich bei der Verwirklichung von Entwicklungs- und Sanitärzielen (zumindest in Ländern mit hohem Einkommen). Die Nachteile der zentralisierten Infrastruktur stellen jedoch ihre Wirksamkeit in Bezug auf die Nachhaltigkeit und die Ausdehnung der Dienstleistungen auf Entwicklungsländer in Frage. Die Hauptnachteile traditioneller Wassernetze werden immer deutlicher: starke Abhängigkeit von großen Wassermengen, ineffiziente Ressourcennutzung, hohe Investitionskosten und langfristige Planungshorizonte (Larsen et al. 2016).

Was die Infrastruktur betrifft, so sind unsere Systeme veraltet und unterfinanziert. In den USA kommt es alle zwei Minuten zu einem Wasserleitungsbruch und täglich gehen schätzungsweise 20 Milliarden Liter aufbereitetes Wasser verloren – genug, um mehr als 9 000 Schwimmbäder zu füllen (ASCE 2021). Die Trinkwassernetze verlieren regelmäßig durchschnittlich 20 - 30 % des durch sie geleiteten Wassers, und diese Zahlen können bei alten Systemen, insbesondere bei solchen, die ineffizient gewartet wurden, auf über 50 % ansteigen (El-Zahab et al. 2019). Die jährliche Investitionslücke bei der Trinkwasserver- und Abwasserentsorgung wird bis 2029 auf 434 Mrd. US-Dollar geschätzt (ASCE 2020). Laut einer aktuellen Erhebung der US Water Environment Federation (WEF 2021) besteht im US-Regenwassersektor eine jährliche Finanzierungslücke von schätzungsweise 8,5 Mrd. US-Dollar. In Deutschland belaufen sich die jährlichen Investitionen für die Kanalsanierung auf etwa fünf Mrd. Euro, während der Kapitalbedarf selbst bei sehr konservativen Annahmen auf mehr als sechs Mrd. Euro geschätzt wird (IPK 2020).

Neben der Finanzierungslücke und dem allgemeinen Zustand der Infrastruktur gibt es erhebliche Hindernisse für eine nachhaltige Wasserwirtschaft. Die zunehmende Verstädterung, neu auftretende Schadstoffe, konkurrierende Wassernutzungen und die Notwendigkeit, Maßnahmen zur Abschwächung der Auswirkungen des Klimawandels zu ergreifen, sind nur einige der Faktoren, die sich auf die Nachhaltigkeit der Dienstleistungen auswirken (Larsen et al. 2016; siehe auch Milman et al. 2021 für eine detaillierte Analyse des Status und der Einschränkungen).

Die Notwendigkeit, Dezentralisierung und ressourceneffiziente Systeme zu erforschen

Die aktuellen Herausforderungen drängen die Betreiber dazu, kostengünstigere und ressourceneffizientere Systeme zu entwickeln, die die gewünschten Wasserdienstleistungen erbringen und gleichzeitig die Einschränkungen des herkömmlichen zentralisierten Systems abmildern. Die aktuellen technologischen Fortschritte (insbesondere in den Bereichen IoT und Modellierung) begünstigen auch die Entstehung neuer hybrider und dezentraler Systeme wie nachhaltige Regenwasserbewirtschaftung, Wasserwiederverwendung, Quellentrennung und dezentrale Aufbereitung (Rabaey et al. 2019). Die folgenden Abschnitte geben einen kurzen Überblick über die aktuellen Trends.

Regenwasserbewirtschaftung

Aufgrund der zunehmenden Verstädterung und der Vergrößerung der versiegelten Flächen in den Städten sind die Grenzen der herkömmlichen Stadtentwässerung im Bereich der Regenwasserbewirtschaftung deutlich geworden. In den letzten

Für einen Überblick über die Herausforderungen und künftigen Veränderungen im Wassersektor

Larsen, T. A., Hoffmann, S., Lüthi, C., Truffer, B., & Maurer, M. (2016) Emerging solutions to the water challenges of an urbanizing world. Science, 352(6288): 928-933.

Jahrzehnten wurden mehrere ökosystembasierte Ansätze zur Renaturierung städtischer Gebiete entwickelt, um die Resilienz städtischer Systeme zu verbessern (Sarabi et al. 2019). Nachhaltige Entwässerungssysteme (SUDS), auch bekannt als „Best Management Practices“ (BMPs), naturbasierte Lösungen (NBS) oder grüne Infrastruktur (GI), wurden als Alternative zur herkömmlichen Ableitung von Regenwasser entwickelt. Heutzutage werden grüne Infrastrukturen weithin als die Zukunft der nachhaltigen Entwässerung angesehen und als Mittel zur Integration dezentraler Wasser- und Abwassersysteme in die herkömmlichen grauen Infrastrukturnetze großer Betreiber betrachtet (Meney et al. 2022). In Europa wird die Begrünung der Städte als wichtiger Hebel zur Erreichung der ehrgeizigen Ziele des Europäischen Green Deal und der Vision der Nullverschmutzung bis 2050 anerkannt (European Commission 2021). In Deutschland werden dezentrale Regenwasserbewirtschaftungsoptionen immer wichtiger, um eine nachhaltige Siedlungswasserwirtschaft zu erreichen. Dazu gehören lokale Maßnahmen wie die Wasserrückhaltung, die Entkopplung versiegelter Flächen vom Abwassernetz sowie die Versickerung, Evapotranspiration und Regenwassernutzung (Geyler et al. 2019). Begrünte Dächer, Becken, Regengärten und urbane Seen werden zunehmend eingesetzt, um das bestehende zentrale System zu ergänzen und zu verbessern. Sie bieten ein deutlich höheres Maß an Flexibilität und gelten als besser geeignet, um sich an künftige Veränderungen anzupassen und mit den durch den Klimawandel verursachten Verunsicherungen umzugehen.
Die Haupthindernisse für die Einführung grüner Infrastrukturen sind jedoch nicht technischer Natur. Die institutionelle Fragmentierung („sektorale Silos“) ist ein bedeutsames Hindernis, da die Umsetzung dezentraler Alternativen die Zusammenarbeit mehrerer Abteilungen im Entscheidungsfindungsprozess erfordert, die ihre eigene Vision, ihren eigenen Rechtsrahmen und ihre eigenen Verfahren haben (Sarabi et al. 2018). Ein weiteres Hindernis ist die Notwendigkeit, die Eigentumsverhältnisse an der Infrastruktur neu zu regeln. So könnten Grundstückseigentümer:innen und eine Vielzahl neuer Interessengruppen die Verantwortung für die Installation, den Betrieb und die Wartung dezentraler Optionen übernehmen und eine wichtige Rolle für das Funktionieren des gesamten Systems spielen (Geyler et al. 2019). Trotz dieser Herausforderungen nimmt die Akzeptanz dezentraler Lösungen zu. Die chinesische Regierung hat sich beispielsweise das Ziel gesetzt, dass bis Ende der 2030er Jahre mehr als 80 % der städtischen Gebiete über Sponge-City-Infrastrukturen verfügen sollen (Qi et al. 2020).

Für eine Analyse der Triebkräfte des Wandels und des Paradigmenwechsels in der Wasserversorgung

Milman, A., Kumpel, E., & Lane, K. (2021) The future of piped water. Water International, 46 (7-8): 1000-1016.

Trennung der Quellen

Die möglichst frühzeitige Trennung von Abwasserströmen ist eine Möglichkeit, die Ressourcenrückgewinnung zu erleichtern und den Behandlungsprozess zu beschleunigen. Die Trennung kann auf Ebene der Haushalte, aber auch auf Ebene eines einzelnen Haushaltsgeräts erfolgen. Die Quellentrennung kann im Allgemeinen als eine Technologie zur Verbesserung der Leistung bestehender Sanitärsysteme dienen. Ihre Rolle beruht auf dem hohen Nährstoffgehalt von Urin: 80 % des Stickstoffs und 50 % des Phosphors im häuslichen Abwasser stammen aus dieser einen Quelle. Durch die Abtrennung des größten Teils des Urins in der Toilette wird das Nährstoffverschmutzungspotenzial des Abwassers stark reduziert und gleichzeitig werden neue Recyclingmöglichkeiten geschaffen, die die Kreislaufwirtschaft unterstützen (Larsen et al. 2021).

In den letzten Jahrzehnten wurden weltweit eine Reihe von Projekten durchgeführt, um Urin vom restlichen Abwasser zu trennen und ihn zu Produkten wie Dünger zu recyceln. Auf der Insel Gotland beispielsweise hat das aus der Schwedischen Universität für Agrarwissenschaften hervorgegangene Unternehmen Sanitation360 eine Lösung entwickelt, um Urin während der Sommertouristensaison in wasserlosen Urinalen auf der ganzen Insel zu sammeln. Sie verwenden ein Verfahren zur Trocknung des Urins zu betonähnlichen Brocken, die sie zu einem Pulver hämmern und zu Düngemittelpellets pressen, die in lokale landwirtschaftliche Geräte passen (Wald 2022). In Paris werden im Rahmen eines Öko-Stadtteilprojekts in einem Gebiet mit 1 000 Einwohner:innen im Stadtzentrum urinaufbereitende Toiletten installiert (Courtois 2020). Die Bill & Melinda Gates Foundation initiierte ein umfangreiches Forschungsprogramm (Re-invent The Toilet Challenge) und investierte Millionen von

US-Dollar, um ein System zu entwickeln, das Urin trennen und gleichzeitig menschliche Ausscheidungen in Strom, Trinkwasser und Dünger umwandeln kann (Gates Foundation o. J.). Abgesehen von diesen vielversprechenden Initiativen ist die Urinseparierung noch immer keine moderne Alternative zu den herkömmlichen Abwassersystemen. Hauptengpässe sind derzeit das Fehlen kostengünstiger industrieller Marktlösungen sowie Probleme mit der richtigen Planung, Installation und Wartung der Systeme vor Ort (Larsen et al. 2021). Durch die Entwicklung neuer Innovationen zur Steigerung der Effizienz der Methode sowie geeigneter Modelle für die Verbreitung, die Kommerzialisierung und den Aufbau von Kapazitäten könnte das Konzept der Trennung nach Quellen enormes Potenzial zur Verbesserung der Effizienz städtischer Wassersysteme bieten.

Dezentralisierte Wasserwiederverwendung

Eine weitere Möglichkeit, die Nachteile des traditionellen Systems auszugleichen, ist die Einführung dezentraler Wasserwiederverwendungssysteme. Die Wiederverwendung von Wasser bezieht sich auf die Verwendung von behandeltem Abwasser in kleineren Wasserkreisläufen als Mittel zur Linderung regionaler Engpässe. Dies kann in Form der Wiederverwendung von Wasser in industriellen Produktionsprozessen und der Verwendung von gereinigtem Abwasser für die landwirtschaftliche Bewässerung geschehen. Israel ist ein führendes Land in diesem Bereich: Seit den 1950er Jahren wird Abwasser für weitere Zwecke wiederverwendet. Heute werden fast 90 % der Abwässer des Landes wiederverwendet, vor allem für die landwirtschaftliche Bewässerung, um die Wasserknappheit zu bekämpfen, die Wassersicherheit zu gewährleisten und mehr als die Hälfte des gesamten landwirtschaftlichen Bedarfs zu decken (Umweltbundesamt 2021). Während große, zentralisierte Anlagen Größenvorteile nutzen können, können kleinere, dezentrale Anlagen inzwischen mit der Effizienz von Großanlagen mithalten und vermeiden gleichzeitig die erheblichen Risiken einer Überbauung (Fluence o. J.). In diesem Zusammenhang stehen dezentrale Wiederverwendungstechnologien dem Konzept der Kreislaufwirtschaft näher und haben das Potenzial, den Kreislauf zwischen Abfall und Ressourcen vor Ort zu schließen. Abwasser ist nicht länger ein Nebenprodukt städtischer Gebiete, sondern wird zu einer Ressource an sich, die Energieeinsparungen, Abfallrecycling und Wassereinsparungen fördert (Grant et al. 2012).

Das Konzept der dezentralen Wasserwiederverwendung hat in den letzten Jahren unter dem Begriff "Sewer-Mining" an Dynamik gewonnen (Makropoulos et al. 2017). Sewer-Mining wird in der Nachbarschaft eingesetzt und beruht auf der Aufbereitung von Wasser aus der lokalen Kanalisation zur Versorgung lokaler nicht trinkbarer Anwendungen (wie z. B. der Bewässerung von Stadtgrün), wobei die Behandlungsrückstände in die Kanalisation zurückgeführt werden. Es werden neue Aufbereitungslösungen entwickelt und IoT-Lösungen eingesetzt, um die Steuerung der Systeme zu verbessern (Karagiannidis et al. 2016). Die Verfügbarkeit von Daten treibt auch die Einführung neuartiger Frühwarnsysteme voran, um bakterielle und toxische Verunreinigungen zu verhindern und die Verwaltung von Wiederverwendungssystemen zu optimieren (Marinelli et al. 2021). Für die Einführung des Sewer-Mining gibt es noch erhebliche Herausforderungen, darunter die öffentliche Wahrnehmung, unzureichende rechtliche Rahmenbedingungen und finanzielle Zwänge. Erforderlich ist einerseits die Entwicklung neuer Aufbereitungsverfahren, die aus Rohabwasser hochwertiges aufbereitetes Wasser erzeugen können und die für eine dezentrale Anwendung simpel und robust genug sind. Andererseits braucht es neue Geschäftsmodelle, um die wirtschaftliche Rentabilität für die Betreiber zu gewährleisten (Makropoulos et al. 2017).

Für ein besseres Verständnis des Echtzeit-Kontrollpotenzials für grüne Infrastrukturen

Brasil, J., Macedo, M., Lago, C., Oliveira, T., Júnior, M., Oliveira, T., & Mendiondo, E. (2021) Nature-based solutions and real-time control: challenges and opportunities. Water, 13 (5): 651.

#2 Risiken

Der vorangegangene Abschnitt hat einen Überblick über die wichtigsten Trends und Möglichkeiten gegeben, die sich durch die Dezentralisierung der Infrastruktur ergeben. Aufgrund der Vielfalt und Komplexität der anstehenden Herausforderungen ist klar, dass es keine Einheitslösung geben wird und dass die Entwicklung der Infrastruktur eher langsamen inkrementellen Verbesserungen als einer disruptiven Transformation folgen wird (Rabaey 2021). Neben den massiven Hindernissen für die Einführung – die natürlich nicht nur technischer Natur sind – wird die Umgestaltung der Infra-

struktur die derzeitige Architektur unserer Systeme verändern und könnte die Quelle für neue Schwachstellen und Sicherheitsprobleme sein.

Die zunehmende Komplexität und Verbreitung des IoT eröffnen neue Sicherheitslücken

Eine der größten Herausforderungen bei der Umsetzung dezentraler Lösungen liegt in der zunehmenden Komplexität des integrierten Systems. Bei der Regenwasserbewirtschaftung zum Beispiel geht es bei dezentralen Ansätzen um die Integration heterogener blau-grüner Infrastrukturen in die konventionellen städtischen Entwässerungssysteme. Allerdings gibt es immer noch Unklarheiten über den angemessenen Grad der Integration und Unsicherheiten über die Effizienz und Funktionsweise der neuen hybriden Infrastrukturen (UNESCO 2018). Auch das Wissen über dezentrale Techniken, einschließlich der richtigen Planung, Konstruktion und Wartung, muss weiter verbessert werden. Die Wartung stellt eine große Herausforderung dar, auch im Hinblick auf die damit verbundenen Kosten (Akther et al. 2018).

Mit den sich abzeichnenden Trends von IoT und Smart Cities werden neue Ansätze erforscht, um solche komplexen Systeme zu überwachen und deren Steuerung zu verbessern (Kerkez et al. 2016, Barthelemy et al. 2020, Strauss et al. 2022). Zu den geplanten Visionen gehören Sensornetzwerke, die Daten in Echtzeit liefern, eine dynamische Steuerung des Flusses und der Qualität von Regenwasser sowie Frühwarnsysteme für Hochwasserrisiken (Shishegar et al. 2021; siehe Brasil et al. 2021, für einen Überblick über das Echtzeitsteuerung -Potenzial für NBS und Prashant Kumar et al. 2021, für eine Übersicht über Überwachungstechniken zur Leistungsbewertung). Die Transformationen im Bereich des Monitorings mit dem Aufkommen kostengünstiger Sensoren, der Miniaturisierung und Open-Source-Schnittstellen sollten den Betreibern auch neue Möglichkeiten für das Management der Komplexität der dezentralen Infrastruktur auf lokaler Ebene bieten (Cherqui et al. 2019). Es wird erwartet, dass dieser Trend durch die Abnutzung von blau-grünen Infrastrukturen beschleunigt wird, die deutlich schneller verlaufen kann als die von traditionellen leitungsgebundenen Infrastrukturen. Dadurch kann die Lernkurve beim Asset Management von blau-grünen Lösungen viel schneller verlaufen als die Jahrzehnte, die für die Entwicklung des Asset Managements von Kanalnetzen benötigt wurden (Langeveld et al. 2022).

Die mit dieser Entwicklung verbundenen Risiken überschneiden sich weitgehend mit den Risiken im Zusammenhang mit der Einführung des IoT, die in Kapitel 2.1 (IoT und intelligente Sensoren) erörtert wurden. Es liegt auf der Hand, dass die Notwendigkeit der Kontrolle grüner Infrastrukturen in Verbindung mit ihrer großen Heterogenität in Bezug auf Art, Umfang und Funktion zu neuen Cyberrisiken führen wird. Betreiber werden anfälliger für Bedrohungen, die darauf abzielen, IT- und OT-Netzwerke sowie einzelne Systeme und Geräte zu kompromittieren.

Der Schutz des sozialen Mehrwerts grüner Infrastrukturen

Eine andere Art von Risiko liegt in der neuen Natur der grünen Infrastruktur, die über die traditionelle Rolle des Abwassersystems für die Wasserableitung, den Schutz der öffentlichen Gesundheit und den Schutz vor Überschwemmungen hinaus, einen Zusatznutzen für die Bürger:innen bietet. Grüne Infrastrukturen bieten eine Reihe von zusätzlichen Vorteilen, die graue Infrastrukturen nicht bieten können, wie z. B. die Schaffung ökologischer Nischen in städtischen Gebieten oder Erholungsgebiete für die Bewohner:innen (Oral et al. 2020). In dicht bebauten Städten wird der Einsatz grüner Infrastrukturen durch deren Zusatznutzen als Hebel zur Verbesserung der Lebensqualität in städtischen Gebieten begünstigt. Aus dieser Eigenschaft könnten sich auch neuartige Risiken ergeben, die direkt mit der Freizeitnutzung und der Integration grüner Infrastrukturen in den öffentlichen Raum zusammenhängen. Angreifer könnten auf Kontrollsysteme abzielen und die Steuerung der Infrastruktur verändern, um lokale Überschwemmungen zu verursachen, die Wasserqualität zu verändern und die wiederhergestellte städtische Biodiversität zu zerstören. Der dezentrale Charakter der grünen Infrastruktur könnte die Auswirkungen eindämmen; die Nähe der Bürger:innen zur technischen Infrastruktur und ihre neue Rolle in der Freizeitgestaltung erfordern jedoch besondere Aufmerksamkeit.

Die Herausforderung des Grundstückseigentums

Das Grundstückseigentum wird häufig als ein großes institutionelles und rechtliches Hindernis für die Einführung grüner Infrastruktur angesehen (Sarabi et al. 2020). Die Unterhaltung grauer Infrastrukturen wird in der Regel direkt von Betreiber und lokalen Behörden verwaltet und beruht auf

klaren Entscheidungsfindungsprozessen. Die Integration grüner Infrastrukturen als Ergänzung zu konventionellen Infrastrukturen erfordert jedoch die Zusammenarbeit mehrerer Interessengruppen, einschließlich der Grundstückseigentümer (Hoang und Fenner 2016). Das Funktionieren dezentraler Infrastrukturen würde nicht nur von einer einzigen Stelle abhängen, sondern von einer Konstellation von Akteuren, die von unterschiedlichen Präferenzen und Zielen geleitet werden. Dieser Wandel beinhaltet eine Verlagerung der Verantwortung für die Installation, den Betrieb und die Instandhaltung grüner Infrastrukturen von dem öffentlichen Betreiber auf die Grundstückseigentümer:innen (Dakhal und Chevalier 2015). Die Auswirkungen dieses neuen Governance-Settings gehen zwar über den Rahmen dieses Berichts hinaus, aber die Verteilung der Verantwortlichkeiten, die zur Erreichung des gewünschten Dienstleistungsniveaus erforderlich ist, könnte die Anzahl der Angriffspunkte erhöhen und die Anfälligkeit des Kontrollnetzes steigern.

Die Verwendung von Luftaufnahmen kann neue Bedenken hinsichtlich des Datenschutzes aufwerfen

Während In-situ-Messungen in der Regel einen hohen Wartungsaufwand und die Zusammenarbeit zahlreicher Akteure erfordern, haben Luftaufnahmen das Potenzial, grüne Infrastrukturen über weite geografische Gebiete, einschließlich städtischer Gebiete, zu überwachen (Kumar et al. 2021). Jüngste Forschungsprojekte haben insbesondere gezeigt, dass Drohnen bedeutende Anwendungen für die Regenwasserbewirtschaftung haben können. Drohnen können in städtischen Gebieten eingesetzt werden, um die Lage von Regenwassereinläufen zu ermitteln (Moy de Vitry et al. 2018) oder mögliche illegale Abwassereinleitungen anhand von thermischen Anomalien in Bächen zu identifizieren (Derrick und Moore 2015). Sie können auch zur Messung der Wasserqualität eingesetzt werden, indem sie während des Fluges Sonden einbetten oder automatisch Proben nehmen (Alam und Manoharan 2017; Koparan et al. 2018). Die Möglichkeit, mehrere Standorte schnell und effizient direkt zu überwachen, würde Betreibern verwertbare Daten liefern, die sie zur Verbesserung der Regenwasserbewirtschaftung nutzen können. Dies könnte auch dazu beitragen, die Ressourcenbeschränkungen klassischer Wasserprobenahmeprogramme zu überwinden (McDonald 2019). Drohnen bieten auch vielversprechende Perspektiven für die Inspektion schwer zugänglicher Regenwasserinfrastrukturen, die sich über eine Vielzahl von Grundstückseigentümer:innenn erstrecken. Diese Art der Anwendung wirft die Frage auf, wie die gesammelten Daten gespeichert, verarbeitet und schließlich genutzt werden können, ohne die Privatsphäre der Bürger:innen zu gefährden.

Die Smart City und die neue Rolle des Wassers

Das Potenzial von Smart Cities

Die Smart City beschreibt ein neues Paradigma der Stadtentwicklung, bei dem durch die Einbettung von digitalen Technologien in das städtische Gefüge und die Vernetzung städtischer Infrastrukturen Siedlungen effizienter und nachhaltiger gestaltet werden (Eremia et al. 2017). Diese Fortschritte sind für Wasserbetreiber besonders wichtig, da sie untrennbar mit einer Vielzahl anderer Infrastrukturen verbunden sind und daher diese Verbindungen nutzen können, um ihre eigenen operativen Fähigkeiten zu verbessern. Durch die vertikale und horizontale Integration städtischer Systeme bietet die Smart City einen übergreifenden Rahmen, innerhalb dessen das Konzept von Wasser 4.0 optimal umgesetzt werden kann.

Der Markt für Smart Cities wächst rasant und wird im Jahr 2030 voraussichtlich einen Wert von 833 Mrd. US-Dollar erreichen (GlobalData 2019). Um eine nachhaltige und inklusive Entwicklung der Städte der Zukunft zu gewährleisten, hat das Bundesministerium des Innern, für Bau und Heimat (BMI) 2018 eine Smart City Charta veröffentlicht. Darin werden Leitlinien formuliert, die den Akteuren helfen sollen, digitale Technologien bestmöglich zu nutzen, um „ressourcenschonende, bedarfsgerechte Lösungen“ für städtische Probleme zu entwickeln und die interkommunale und sektorübergreifende Zusammenarbeit zu fördern. Die vier Hauptbedürfnisse, die in dieser Charta formuliert werden, beziehen sich auf Strategie, Beteiligung, Infrastruktur und Ressourcen. Darüber hinaus wurden vom BMI Fördermittel in Höhe von mehr als einer Mrd. Euro zur Verfügung gestellt, um 73 Städte und Gemeinden bei der Entwicklung von Smart-City-Pilotprojekten zu unterstützen, deren Ergebnisse von einer zentralen Koordinierungs- und Transferstelle koordiniert und gemeinsam genutzt werden sollen. Damit wurde der Stand der Technik in deutschen Smart Cities, der sich bis dahin auf München, Köln, Hamburg und Leipzig konzentriert hatte, deutlich vorangetrieben (Gaia-X 2021).

Auch wenn einige unserer Interviewpartner:innen bereits Kooperationsprojekte mit anderen städtischen Infrastrukturen entwickeln, steht der Wassersektor im Allgemeinen nicht an der Spitze solcher Bestrebungen. Intelligente Städte stützen sich unmittelbar auf die Digitalisierung und das Internet of Things, beides Bereiche, in denen der Wassersektor zurückbleibt. Jedoch lässt sich in Deutschland innerhalb der letzten sieben Jahre eine wachsende Anzahl an konkreten Smart City Umsetzungsprojekten verzeichnen. Es kann also davon ausgegangen werden, dass solche Ansätze auch im Wassersektor an Bedeutung gewinnen werden, besonders hinsichtlich Entwicklungen der Netzinfrastrukturen (Umweltbundesamt 2021). Daher müssen ganzheitliche Strategien entwickelt werden, die nicht nur die technische und organisatorische digitale Transformation der Wasserbetreiber unterstützen, sondern auch ihre übergreifende Integration in städtische Systeme.

Für einen Überblick über Herausforderungen, Chancen und Vorteile bei der Entwicklung integrierter Multi-Utility-Dienstleister

Stewart, R. A. et al. (2018) Integrated intelligent water-energy metering systems and informatics: Visioning a digital multi-utility service provider. Environmental Modelling & Software, 105: 94-117.

Städtische Datenplattformen: der Grundstein für die intelligente Stadt

Um die Smart City zu ermöglichen, werden städtische Datenplattformen benötigt, in denen Informationen aggregiert, standardisiert und geteilt werden. Diese Perspektive bildet die Grundlage für alle anderen in diesem Abschnitt vorgestellten Anwendungen, indem sie den Wassersektor in einen Rahmen der Interoperabilität einbettet. Durch die Kombination heterogener Datensätze, die von verschiedenen Stellen bereitgestellt werden, ermöglichen städtische Datenplattformen die Entwicklung neuer Programme und Anwendungen, die das städtische Geflecht grundlegend verändern können (Schieferdecker et al. 2016). Die Landschaft der städtischen Datenplattformen ist recht vielfältig, wobei einige vollständig offene Datenbestände enthalten und andere sogar integrierte Marktplätze oder Beteiligungsplattformen eingebaut haben.

Im Rahmen der deutschen Smart-City-Modellprojekte entwickelt die Stadt Potsdam eine städtische Datenplattform, nicht nur um die gemeinsame Nutzung städtischer Daten und Anwendungen voranzutreiben, sondern auch den öffentlichen Dialog und Beteiligung zu ermöglichen und somit die Akzeptanz für neue städtische Lösungen zu fördern (Potsdam o. J.). Weitere Beispiele für städtische Datenplattformen in Deutschland sind die zentrale

offene Datenplattform von Paderborn (Digitale Heimat Paderborn 2019) oder die offene Datenplattform von Hamburg (Hamburg o. J.).

Der wachsende Bedarf an Dateninteroperabilität

Interoperabilität ist ein wesentlicher Faktor für den Erfolg einer intelligenten Stadt, denn ohne sie kann die sektorübergreifende Zusammenarbeit nicht über lokalisierte Lösungen hinausgehen und die Erzielung von Skaleneffekten wird deutlich erschwert. Dieser Mangel an Interoperabilität erhöht nicht nur die Betriebskosten und verringert den Wert der Daten, da sie bei jeder Wiederverwendung neu verarbeitet werden müssen, sondern erhöht auch das Risiko, in eine Anbieterbindung (Vendor-Lock-in) zu geraten (Jeong et al. 2020). Umgekehrt ermöglicht die Schaffung gemeinsamer Protokolle für die Interoperabilität den Aufbau einer umfassenden gemeinsamen Datenplattform, aus der grundlegend neue Erkenntnisse gewonnen werden können. Darüber hinaus würde ein solcher Rahmen auch die Aktualisierung von Datensätzen erheblich erleichtern, indem zugängliche Pfade für eine direkte Verbindung zu IoT-Umgebungen geboten werden. Innerhalb dieses Ökosystems ist es sogar möglich, Marktplatzfunktionen hinzuzufügen, so dass Datensätze einfach verwaltet und erworben und – über komplexere Cloud-Infrastrukturen – sogar innerhalb derselben Plattform analysiert werden können. Die drei wichtigsten Faktoren für eine erfolgreiche Smart-City-Datenplattform sind: Standards (zur Gewährleistung der Interoperabilität), Offenheit (zur Gewährleistung des Zugangs und der dynamischen Entwicklung) und Modularität (zur Gewährleistung der Erweiterungsmöglichkeit) (Jeong et al. 2020).

Einen solchen Ansatz verfolgt FIWARE. Ziel ist, technische, wirtschaftliche und soziale Innovationen voranzutreiben. FIWARE ist eine cloudbasierte IoT-Plattform, die von der Europäischen Kommission gefördert wird und aus einem interoperablen, offenen Datenökosystem besteht. FIWARE trägt insbesondere dazu bei, eine Reihe von Standarddatenmodellen und Kommunikationsprotokollen zu entwickeln, um sektorübergreifende digitale Lösungen zu erleichtern und die Übertragbarkeit intelligenter Lösungen zwischen Städten zu fördern. FIWARE wird auch zunehmend im Wassersektor eingesetzt. So hat das Projekt FIWARE4WATER kürzlich einen bereichsübergreifenden Datenaustausch und eine kooperative Multi-Stakeholder-Plattform entwickelt, mit der neue modulare Anwendungen für alle Phasen des Wasserkreislaufs entwickelt werden können (Fiware4Water o. J.-a, Fiware4Water o. J.-b).

Ergänzend zur FIWARE-Initiative zielt Gaia-X (siehe Kapitel 2.3) ebenfalls auf die Schaffung einer neuen Generation von Dateninfrastrukturen ab, die allerdings auf einzelne Cluster spezialisiert sind. Eines dieser Cluster ist „Smart City / Smart Region“, das darauf abzielt, eine standardisierte Cloud-Netzwerkinfrastruktur auf europäischer Ebene zu fördern, die mit gemeinsamen Standards für die Interoperabilität verbunden ist. Dabei liegt der Fokus darauf, dass Lösungen leicht anpassbar sind, Daten schnell nutzbar sind und der Betrieb digitaler Infrastrukturen deutlich günstiger wird (Gaia-X 2021). Um diese Ziele zu erreichen, umfasst das Gaia-X-Projekt auch einen Katalog von Best Practices, der (Meta-) Daten-Cybersicherheitsstandards und semantische Standards zur Gewährleistung der Interoperabilität enthält. Darüber hinaus übernimmt die Gaia-X-Umgebung auch eine unterstützende Rolle, indem sie Reifegradbewertungen durchführt, Datenkompetenzen vermittelt und Leitlinien für übergreifende Digitalisierungsstrategien formuliert (Gaia-X 2021).

Für einen Überblick über europäische Initiativen zur Entwicklung von städtischen Datenplattformen und Interoperabilitätsstandards

Gaia-X (2021) Domäne Smart City / Smart Region; Positionspapier Version 1.0 2021.

Städtische Datenplattformen und der dazugehörige Rahmen für die Interoperabilität sind die Grundvoraussetzungen für erfolgreiche Smart-City-Umgebungen. Auf der Grundlage dieses Datenökosystems können städtische Betreiber ihre eigenen datengesteuerten Strategien ausarbeiten, um neue Anwendungen zu entwickeln und ihre Dienstleistungen zu optimieren. In diesem Zusammenhang wird der Wassersektor eine der bestimmenden Komponenten zukünftiger Smart Cities sein, da die von ihm verwalteten Ressourcen für jeden Akteur auf jeder Ebene wesentlich sind. Insbesondere bei der Bewältigung globaler Herausforderungen, wie z. B. Klimawandel oder Umweltverschmutzung, werden sich Innovationen in der Wasserinfrastruktur und ihren transversalen Anwendungsfällen als entscheidend erweisen. Obwohl solche Maßnahmen

in der Wasserversorgung noch nicht weit verbreitet sind, werden im folgenden Abschnitt einige Projekte der sektorübergreifenden Zusammenarbeit beispielhaft vorgestellt, um die erheblichen Fortschritte zu veranschaulichen, die durch Smart Cities ermöglicht werden. Allerdings haben nicht alle Sektoren das gleiche Kooperationspotenzial.

Die Rolle des Wassers in der Smart City

Energie:
Es wird erwartet, dass die Zusammenarbeit mit dem Energiesektor die Nachhaltigkeit der Wasserdienstleistungen verbessert, indem sie eine Senkung des Energieverbrauchs sowie Maßnahmen zur Energieerzeugung ermöglicht. Intelligente Zähler und intelligente Netze sind ein Paradebeispiel für ein übergreifendes Konzept für Energie und Wasser. Da diese Betreiber sowohl in Bezug auf die Versorgung als auch auf die Endnutzung eng miteinander verbunden sind und vor ähnlichen Herausforderungen stehen, könnte eine verstärkte Zusammenarbeit zu neuen und verbesserten Lösungen für beide Branchen führen, und zwar nicht nur in technischer, sondern auch in organisatorischer und unternehmerischer Hinsicht (Young 2013). Die Zusammenarbeit dieser beiden voneinander abhängigen Ressourcen steigert nicht nur die Effizienz und minimiert die wirtschaftlichen und ökologischen Belastungen, sondern erhöht auch das übergreifende Wissen und verbessert die Sicherheit und Verfügbarkeit beider Branchen und trägt zur Bekämpfung von Kaskadeneffekten bei (Young 2013).

Eine urbane Anwendung der Verbindung des Wasser- und Energiesektors ist das intelligente Heizen und Kühlen, ein Beispiel dafür findet sich in Amsterdam. Dort werden im Rahmen eines von city-zen durchgeführten Projekts jährlich 1 815 Tonnen Kohlenstoff eingespart, indem die Kälte aus den Trinkwasserleitungen entnommen und zur Kühlung der Sanquin-Blutbank verwendet wird. Dadurch wird gleichzeitig die Energiemenge reduziert, die die Bewohner:innen für das Erhitzen des Wassers aufwenden müssen (City-zen 2019).

Verkehrswesen:
Die wichtigsten Fortschritte bei der Zusammenarbeit mit dem Verkehrssektor liegen vor allem im Bereich des Wetter- und Hochwassermanagements und einer optimierten Verwaltung der negativen Wechselbeziehung zwischen Wasser- und Verkehrsinfrastrukturen. Eines der innovativsten Projekte in diesem Bereich ist SENSARE, eine Plattform, die ein Frühwarnsystem bereitstellt, das meteorologische und topografische Daten integriert, um zivile Sicherheitsorganisationen mit einschlägigen Daten zu versorgen. Dies ermöglicht die Sperrung überschwemmungsgefährdeter Gebiete, Verkehrsumleitungen und eine allgemeine Verbesserung des Verkehrs für alle Teilnehmer:innen (Neumann et al. 2021). Durch die Identifizierung von Risikogebieten und die Erstellung eines Simulationsmodells für den Oberflächenabfluss können Sensoren zur Echtzeitüberwachung von Überschwemmungsereignissen installiert werden, die eine wesentlich schnellere Reaktion von Schutzmaßnahmen ermöglichen.

Gebäude und Smart Homes:
Der unmittelbar einleuchtende Fall einer stärkeren Integration der Wasserbetreiber in Haushalte und Gebäude ist die intelligente Verbrauchsmessung, die einen bilateralen Informationsfluss ermöglicht. Dies würde zum einen den Verbraucher:innen helfen, ihren Wasserverbrauch zu überwachen, zu verstehen und zu reduzieren, und zum anderen den Versorgern helfen, genauere Wasserbedarfsprofile zu erstellen und bessere Schätzungen und Prognosen zu machen. Durch die Modellierung des Wasserverbrauchs pro Gebäude, pro Wohnung, pro Gerät oder pro Nutzer:in können die Versorger die Verbrauchsdaten kontextualisieren und die Wartung und Bereitstellung von Dienstleistungen weiter optimieren, beispielsweise durch adaptive Preismaßnahmen (Rodriguez-Diaz et al. 2015, Howell et al. 2017).

Stadtplanung:
Die Wasserinfrastruktur kann auch auf einer übergeordneten Ebene mit dem Siedlungsbau verknüpft werden, indem die Projekte auf Nachbarschafts- oder sogar Stadtteilebene entwickelt werden, ein breiteres Spektrum von Akteuren einbeziehen und über technische Maßnahmen hinausgehen, um auch Fragen der Governance zu beeinflussen.

Für eine Vertiefung der Risiken, Herausforderungen und Lösungen zu sicheren Smart City Frameworks

Khan, Z. et al. (2017) Towards a secure service provisioning framework in a smart city environment. Future Generation Computer Systems 77: 112-135.

Das Projekt „Amsterdam Rainproof“ ist ein großes Netzwerk verschiedener Interessengruppen, die zusammenarbeiten, um den Wasserhaushalt und die Nachhaltigkeit in Amsterdam zu verbessern. Ein Teil davon besteht darin, die Menschen zu mobilisieren, die Regenwasserbewirtschaftung in ihren Häusern und Nachbarschaften zu verbessern. Beispiele für Gebäude sind begrünte Polderdächer in renovierten Wohnkomplexen (Vesteda) oder Büros (Breevast). Beispiele für Wohnungen sind Selbstbau-Maßnahmen zum Schutz vor Überschwemmungen (De Baarsjes-Viertel), der Umbau und die Anpassung von Lagerkomplexen (BloemDwars-Projekt) und das Sammeln von Regenwasser (Buiksloterham-Viertel). Im Einklang mit dem Trend zu dezentralen Infrastrukturen können Smart Cities die Zusammenarbeit auf Mikroebene unterstützen, indem sie Praxisgemeinschaften bilden, die den städtischen Raum umgestalten und die Umsetzung nachhaltiger Maßnahmen wie intelligente Dächer, intelligente Regentonnen oder Sickerpflaster fördern. Durch pädagogische Maßnahmen kann das öffentliche Interesse an nachhaltiger Wassernutzung geweckt und die Wasserinfrastruktur einer Stadt dauerhaft verbessert werden (Amsterdam Rainproof o. J., Amsterdam Rainproof 2016).
Die Verknüpfung von Stadtplanung und Wassermanagement ist ein Schlüsselelement des kürzlich im Zuge der „Modellprojekte Smart Cities“ geförderten Smart Water Projekts in Berlin. Mit diesem Projekt will Berlin neue Simulations- und Kollaborationswerkzeuge entwickeln, um die Integration von grüner Infrastruktur für die Regenwasserbewirtschaftung in Stadtplanungsprojekte zu unterstützen. Insbesondere wird die Verwaltung eine Webanwendung für Bürgerinnen und Bürger bereitstellen, um das Potenzial verschiedener Regenwasserbewirtschaftungsszenarien zu visualisieren und über positive Auswirkungen auf den Gewässerschutz, den Hochwasserschutz und die Klimaanpassung zu informieren (BMI 2020).

Risikomanagement und Katastrophenschutz:
Die Verfügbarkeit offener Daten aus einer Reihe von Sektoren auf städtischen Datenplattformen bildet die Grundlage für die Entwicklung datengestützter Risikomanagement-Tools. Ein solches Beispiel ist das Operations Centre aus Rio de Janeiro, das teilweise als Reaktion auf die massiven Überschwemmungen, von denen die Stadt 2010 betroffen war, eingerichtet wurde. Es sammelt und überwacht nicht nur große und heterogene städtische Datensätze, sondern dient auch dazu, alle Versorgungseinrichtungen und Notdienste der Stadt miteinander zu verbinden. Durch die Zusammenführung von meteorologischen und topografischen Daten, Stadtplanungsprojekten, Social-Media-Analysen und einer zentralen Überwachungsstation, die rund um die Uhr von mehr als 40 städtischen Behörden betrieben wird, können Überschwemmungsereignisse verhindert bzw. erkannt werden und der Öffentlichkeit in Echtzeit mitgeteilt werden (Luque-Ayala und Marvin 2016).

#2 Risiken

Der zunehmende Informationsaustausch in der Smart City bringt zwangsläufig erhöhte Risiken und Bedenken in Bezug auf Datensicherheit und Datenschutz mit sich. Insbesondere die enorme Größe, Komplexität, Heterogenität und Dynamik der Datenökosysteme von Smart Cities machen die Durchführung von Risikobewertungen und die Entwicklung umfassender Cybersicherheitsstrategien äußerst schwierig. Die Erfassung, Speicherung und Übermittlung von Daten aus Smart-City-Infrastrukturen stellt eine ständige Sicherheitsbedrohung dar (Ismagilova et al. 2020). Die Zahl der Cyberangriffe nimmt zu und die zunehmende Konnektivität der Smart City führt zu einer erhöhten Anfälligkeit.

Datenschutz

Abgesehen von der allgemeinen Sorge, dass personenbezogene Daten durchsickern oder gestohlen werden könnten, was durch die schiere Menge der in einer Smart-City-Umgebung gesammelten Daten noch wahrscheinlicher wird, erhöht die Tatsache, dass die Daten mehrerer Betreiber zentral zusammengefasst werden, die Gefahr des Diebstahls personenbezogener Daten. Nicht nur der Wasser- oder Energieverbrauch, sondern auch der Standort (aus dem Verkehr), der Gesundheitszustand (aus dem Gesundheitswesen) oder sogar der Lebensstil und das Verhalten (aus Smart Homes und als Aggregat aus anderen Bereichen) können aus gestohlenen Datensätzen abgerufen oder abgeleitet werden (Zhang et al. 2017). Der Datenschutz ist nicht nur ein Problem im Zusammenhang mit böswilligen Cyberangriffen, sondern auch in Bezug auf die Interoperabilität innerhalb der Smart City. Die Frage, welche Betreiber Zugang zu welchen Daten in Bezug auf Speicherung, Verarbeitung und Analyse haben, muss sorgfältig geprüft werden. Vertrauen wird zu einem entscheidenden Merkmal für den Erfolg der Smart City (Ismagilova et al. 2020).

Kaskadeneffekte und die Übertragung von Sicherheitsbrüchen

Die vernetzten Infrastrukturen von Smart Cities erhöhen nicht nur die Wahrscheinlichkeit und das Ausmaß von schädlichen Kaskadeneffekten, sondern führen auch dazu, dass Sicherheitsverletzungen im Netz eines Betreibers automatisch eine Bedrohung für andere Betreiber darstellen (Kalinin et al. 2021). Die Komplexität der Smart City erhöht die Schwierigkeit und die Kosten für die Umsetzung geeigneter Sicherheitsmaßnahmen, und die zentralisierten Datenplattformen sowie die Rechenzentren, auf die sich diese Stadtform stützt, erweisen sich als wertvolle Ziele für Cyberangriffe.

Die zunehmende Heterogenität und Komplexität der vernetzten Systeme

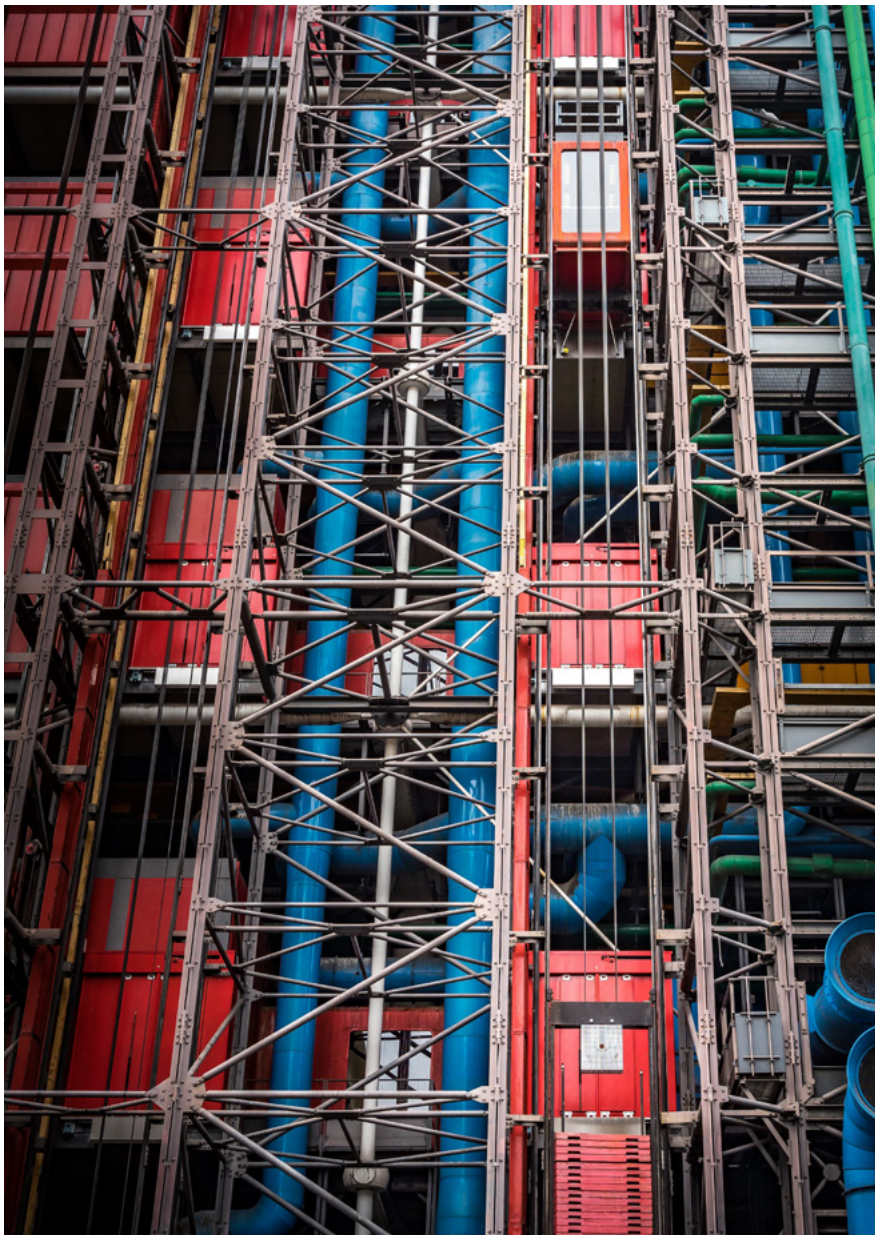
Die schiere Anzahl heterogener Anlagen verschiedener Betreiber, die sich in Bezug auf Hardware, Software, Hersteller und Standards unterscheiden, sowie die Vielfalt der horizontalen Verbindungen und die sich ständig ändernden Netztopologien machen es „unmöglich, eine zentralisierte Sicherheitsstrategie zu organisieren“. Ohne angemessene Cybersicherheitsmaßnahmen für die einzelnen Netzknoten bedeutet der öffentliche Charakter des Netzes außerdem, dass es viel einfacher ist, sich Zugang zu einem potenziell anfälligen Knoten zu verschaffen. Diese Knoten leiden unter denselben Cybersicherheitsschwächen wie die im IoT (siehe Kapitel 2.1) genannten, wo sie aufgrund ihrer begrenzten Rechenleistung sehr leicht zu hacken oder zumindest Daten zu stehlen sind (Kalinin et al. 2021).

Handlungs-empfehlungen

Aufbauend auf den im Zusammenhang mit der Digitalisierung des *W*assersektors identifizierten Trends und Risiken, *w*erden 14 konkrete Forschungs- und Ent*w*icklungsbedarfe aufgezeigt. *W*ir hoffen, dass diese Perspektiven die Betreiber und den gesamten *W*assersektor auf ihrem *W*eg zu *w*ider-standsfähigeren und cyber-sicheren *W*asserinfrastrukturen unterstützen *w*erden.

Inhalt

Forschungs- und Entwicklungsbedarf



Dieser Exkurs in die potenzielle Entwicklung des Wassersektors hat die tiefgreifenden Veränderungen und Risiken aufgezeigt, mit denen sich die Betreiber der Zukunft auseinandersetzen müssen, um ihrer Verantwortung als kritische Infrastruktur gerecht zu werden. Ausgehend von der Art der Trends, den damit verbundenen Risiken und dem aktuellen Stand der Cybersicherheitslösungen leiten wir 14 konkrete Forschungs- und Entwicklungsbedarfe ab. In den folgenden Unterabschnitten werden die damit verbundenen Forschungsfragen und einige vielversprechende Forschungsbereiche kurz erläutert.

#1 Verbesserung der Sicherheit von IoT-Komponenten (Link zum Trend: IoT und intelligente Sensoren)

- Wie lassen sich intelligente Sensoren schützen?
- Wie schützt man die zentralisierte Kontrollinstanz des IoT?
- Wie lässt sich ein ganzheitlicher Cybersicherheitsrahmen entwerfen, der die Heterogenität der Komponenten und Kommunikationsprotokolle bewältigen kann?

Das Internet of Things (IoT) bildet die Grundlage für künftige Entwicklungen der Wasserinfrastruktur. Durch die Einbettung intelligenter Sensoren in unsere Umwelt kann eine Fülle von Daten in Echtzeit generiert und übertragen werden, was eine tiefgreifende Veränderung des Umfangs und der Komplexität der Anwendungen und der Effizienz des Wassersektors ermöglicht und seine Nachhaltigkeit erheblich verbessert (Koo et al. 2015, Baanu und Babu 2021). Die schiere Anzahl der Komponenten und Kommunikationsverbindungen, aus denen sich die IoT-Umgebung zusammensetzt, birgt jedoch eine Fülle von möglichen Sicherheitslücken. Um das optimale Funktionieren von IoT-Netzwerken zu gewährleisten, ist weitere Forschung zu speziellen Sicherheitsprotokollen für die Sensorik, zu einer sichereren Infrastruktur für IoT-Server und zu robusten Cyberschutzstrategien, die auch eine schnelle Wiederherstellung von Betriebsschäden gewährleisten können, erforderlich (Jan et al. 2021).

Eine der größten Herausforderungen bei IoT-Netzwerken ist die Implementierung von Cybersicherheitsmaßnahmen in intelligenten Sensoren, da deren Komplexität begrenzt ist. Besonders in diesem Kontext erfordert die Bedingung, dass die Sensoren kostengünstig und verbrauchsarm sein müssen, weitere Forschung, insbesondere zu vielversprechenden Lösungen wie Physical Unclonable Functions (PUF) (Xu et al. 2014, Shamsoshoara et al. 2020).

Hinzu kommt das grundsätzliche Problem, dass die IoT-Infrastruktur eine Vielzahl heterogener Technologien aufnehmen muss und die Entwicklung eines allumfassenden Sicherheitsrahmens eine enorme Herausforderung darstellt. Hier haben sich einige Lösungen herauskristallisiert, wie SDN, FRESCO, OrchSec oder IOT@Work. Das Software Defined Networking (SDN) ist eine verbesserte IoT-Infrastruktur, die die Sicherheitsmängel herkömmlicher Architekturen ausgleicht (Mishra et al. 2020). FRESCO ist ein auf dem OpenFlow-Standard basierendes Framework für die Entwicklung von Sicherheitsanwendungen, das ein schnelles und modulares Design von Erkennungs- und Entschärfungsmodulen mit minimalem Overhead und über 90 % weniger Codezeilen unterstützt, was es ideal für das Prototyping macht (Shin et al. 2013). OrchSec ist eine Orchestrator-basierte Architektur, die eine flexible Umgebung für die Entwicklung von Sicherheitsanwendungen mit reduziertem Overhead bietet, indem Kontrollfunktionen von Überwachungsfunktionen und die Anwendungsentwicklung vom SDN-Controller entkoppelt werden (Zaalouk et al. 2014). Als Alternative zu Autorisierungsprokotollen, die auf Zugriffskontrolllisten basiert sind und deren mangelnde Skalierbarkeit für eine IoT-Umgebung ungeeignet ist, bietet IOT@Work ein fähigkeitsbasiertes Autorisierungs-Framework, das einen Plug-and-Play-Ansatz für Ressourcen und Objekte in IoT-Netzwerken ermöglicht (Khan et al. 2017). Nichtsdestotrotz sind mehr und neuere Lösungen erforderlich, sodass dieser Aspekt in der Forschung besonders priorisiert werden muss.

Schließlich erfordern Wiederherstellungsstrategien bessere Lösungen, die eine permanente Aufrechterhaltung von sicheren und zuverlässigen System-Snapshots garantieren, die ihrerseits verbesserte Sicherheitsmaßnahmen erfordern, um zu gewährleisten, dass die Daten nicht manipuliert werden. Um die Vertraulichkeit der Daten zu

Für einen Überblick über den Stand der Technik von Cybersicherheitslösungen sowie über spannende Forschungsfelder für die Zukunft

Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2021) A systematic review of the state of cyber-security in water systems. Water, 13 (1), 81.

verbessern, können starre Authentifizierungsmechanismen und systematische Vertrauensmodelle sowie Sandboxing-Techniken eingesetzt werden, aber auch die Entwicklung autonomer Vertrauensmechanismen und neuer und verbesserter Datenschutzsoftware muss weiter erforscht werden (Mishra et al. 2020).

#2 Aufbau KI-basierter fortschrittlicher Analysen für Cybersicherheitsprobleme (Link zum Trend: KI)

- Wie können wir datengesteuerte Intrusion Detection Systems (IDS)-Lösungen in OT-Netzen effektiv einsetzen?
- Wie lässt sich die Leistung bestehender Analyseverfahren wie Deep Learning, Clustering und neuronale Netze verbessern und vergleichen?
- Wie kann der Netzwerkverkehr von industriellen Kontrollsystemen (ICS) zusammen mit Prozessdaten bei der Entwicklung von IDS berücksichtigt werden?

Es wird erwartet, dass KI eine Schlüsselrolle für die Cybersicherheit im Wassersektor und insbesondere für den Schutz von OT-Netzen spielen wird (Bhamare et al. 2020). In jüngster Zeit wurden zahlreiche KI-Lösungen entwickelt, um Cybersicherheitsprobleme wie die Analyse von Einbruchserkennungen anzugehen (Lin et al. 2015, Anton et al. 2019). Speziell für Wassernetze wurden bereits mehrere Ansätze getestet, um anormales Verhalten in ICS zu erkennen (Tuptuk et al. 2019). So haben Zou et al. (2019) ein Modell zur Erkennung von Ereignissen entwickelt, das auf Support Vector Machine (SVM) und Online-Messungen der Wasserqualität basiert. Eine zentrale Herausforderung wird darin bestehen, die relevanten Daten (z. B. Angriffsmuster in Zeitreihen für Wasserqualität, Durchfluss, Anlage und Prozessdaten, usw.) zu ermitteln, zu sammeln und zu integrieren, um diese Art von Anwendungen zu trainieren. Eine weitere Herausforderung wird der Umgang mit fehlenden Daten und deren Auswirkungen auf das Training und Leistung von Algorithmen sein. Schließlich müssen neue Modelle entwickelt werden, die der Vielfalt und Vielzahl von Datenquellen zur Verfolgung von Cyberangriffen Rechnung tragen. So wären beispielsweise neue Methoden zur Analyse des Echtzeit-Netzwerkverkehrs von ICS erforderlich, um entlang von Anomalien Bedrohungen bei der Überwachung von Wassermenge und -qualität zu erkennen (Ghaeini et al. 2019). In diesem Bereich besteht eine zentrale Zukunftsherausforderung darin, Erkennungsansätze zu vergleichen, um ihren Mehrwert zu ermitteln und die Relevanz verschiedener Datensätze für die Erkennung von Sicherheitsbedrohungen zu bewerten (Tuptuk et al. 2019).

#3 Erfassung des realen Verhaltens von Analyst:innen bei der Entwicklung von KI-Algorithmen (Link zum Trend: KI)

- Wie lässt sich das Wissen von Cybersicherheits-Analyst:innen in KI-Algorithmen integrieren?
- Wie kann man das Verhalten von Analyst:innen erfassen und diese Daten in KI-Algorithmen einspeisen?

KI kann eingesetzt werden, um tägliche Aufgaben zu automatisieren und Cybersecurity-Analyst:innen dabei zu unterstützen, in Echtzeit auf Ereignisse zu reagieren. Da sich die Cybersicherheit ständig weiterentwickelt, muss KI in der Lage sein, das Verhalten und die Strategien von Analyst:innen kontinuierlich zu erfassen, einschließlich der Erfolge und Misserfolge, um sich an neue Taktiken anzupassen, sobald diese erfunden werden (Bresniker et al. 2019).

Wettbewerbe wie der BATADAL-Wettbewerb (BATtle of the Attack Detection Algorithms), der vom iTrust-Zentrum in Singapur organisiert wird (Taormina et al. 2018), können nützliche Instrumente sein, um unser Verständnis der Mechanismen von Cyberangriffen sowie der Methoden und Strategien von roten und blauen Teams zu verbessern. Die Entwicklung großer gemeinsamer Datensätze für Wasserbetreiber und kritische Infrastrukturen ist eine weitere Möglichkeit, die notwendigen Daten zu sammeln, um das Verhalten von Cybersicherheits-Analyst:innen auf standardisierte Weise zu erfassen und ihre Verhaltensweisen und Strategien aufzuzeichnen. Dieser Ansatz würde den Wissensaustausch fördern und sicherstellen, dass die von den Wasserversorgern eingesetzten KI-Tools ausreichend trainiert sind, um mit dem Stand der Technik in der Cybersicherheit Schritt zu halten.

Die KI-gestützte Verhaltensanalyse ist ein vielversprechender Forschungsbereich, der darauf abzielt, auch das Verhalten von Menschen und nicht nur von Maschinen vorherzusagen. Dieser Ansatz erkennt an, dass die Komplexität von Sicherheitsproblemen Modelle erfordert, die in der Lage sind, Sicherheit als soziotechnisches Phänomen zu artikulieren und zu untersuchen, sowie menschliches Verhalten und die Interaktion mit

technischen Systemen innerhalb einer Organisation zu berücksichtigen (Coles-Kemp und Hansen 2017). Solche Entwicklungen könnten dazu beitragen, anomale Verhaltensweisen über die Überwachung der Reaktion technischer Systeme hinaus zu erkennen, z. B. durch die Verfolgung ungewöhnlicher Mitarbeiteraktivitäten zu ungewöhnlichen Nachtzeiten oder unerwarteter Spitzen bei der Übertragung sensibler Daten (Stevens 2020).

#4 Die Einschränkungen der KI reduzieren und die Robustheit der Vorhersagen erhöhen (Link zum Trend: KI)

- Wie lässt sich die Zuverlässigkeit von KI-Lösungen erhöhen?
- Wie lassen sich kosteneffiziente Lösungen zur Kontrolle von KI-Verhaltensweisen entwickeln?

Neben dem vielversprechenden Einsatz von KI zur Bewältigung von Cybersicherheitsaufgaben ist Forschung erforderlich, um die Grenzen der KI zu überwinden und die Einführung neuer Schwachstellen in die kontrollierten Systeme zu vermeiden. KI kann Gegenstand von Data Poisoning (Biggio 2018) sein, bei dem Angreifer fehlerhafte Daten einbringen, um die Ergebnisse der KI leicht zu verändern und das datengesteuerte Entscheidungsverfahren zu beeinflussen. Diese Angriffe sind heimtückisch und können aufgrund der Natur der KI schwer zu erkennen sein. So kann beispielsweise eine wiederkehrende Bedrohung mit geringen Auswirkungen auf einen KI-Algorithmus als Abweichung in der Leistung der KI und nicht unbedingt als Bedrohung analysiert werden.

Zukünftige Forschung ist erforderlich, um die Zuverlässigkeit von KI-Lösungen zu gewährleisten und einen klaren Rahmen für die Daten-Governance bei ihrer Nutzung zu schaffen (z. B. die Definition von Kontrollverfahren). Eine unzureichende Zuverlässigkeit von KI bedeutet, dass die Technologie zwar Cybersicherheitsaufgaben erfüllen kann, dass aber das Risiko, dass die Lösung versagt oder sich anders als erwartet verhält, zu hoch ist, um sie die Aufgabe ohne jegliche Form der Kontrolle erledigen zu lassen (Taddeo 2019). Um die Zuverlässigkeit von KI zu erhöhen, müssen neue Formen der Kontrolle und ein tiefes Verständnis des Verhaltens von KI-Lösungen entwickelt werden (z. B. parallele Überwachung mit einem KI-Klon). Adversariales Training sollte als eine Möglichkeit erforscht werden, die Leistung von KI zu verbessern, indem Rückkopplungsschleifen mit gegnerischen Beispielen verwendet werden, d. h. Eingaben, die mit dem Ziel erstellt werden, die trainierte KI zu verwirren oder in die Irre zu führen (Carlini und Wagner 2017).

#5 Verbesserung des Verständnisses für neue Sicherheitsfragen im Zusammenhang mit der Konvergenz von IT- und OT-Systemen (Link zum Trend: Cloud-Migration)

- Was sind die Hauptvor- und -nachteile der Konvergenz von IT- und OT-Systemen?
- Wie ist das Nutzen-Risiko-Verhältnis von Cloud-Lösungen für den Wassersektor?

Die kürzlich von UP KRITIS (2020) veröffentlichten Empfehlungen zur Nutzung von Cloud-Diensten in kritischen Infrastrukturen besagen, dass auch kritische Infrastrukturen unter bestimmten Bedingungen Cloud-Dienste nutzen und von den Vorteilen der innovativen Technologie profitieren können. UP KRITIS fasst die wichtigsten Vorteile von Cloud-Lösungen zusammen, unterstreicht aber auch die Notwendigkeit, die durch die Cloud-Nutzung neu entstehenden Risiken (z. B. technische Probleme beim Cloud-Betreiber) effizient anzugehen, und erinnert daran, dass die Verfügbarkeit des kritischen Dienstes durch Cloud-Dienste nicht beeinträchtigt werden darf und voll in der Verantwortung des Betreibers bleibt. UP KRITIS empfiehlt auch die Einrichtung einer übergreifenden Arbeitsgruppe des KRITIS-Betreibers, um konkrete Empfehlungen auf der Grundlage bestehender Standards (z. B. ISO, BSI) und sektorspezifischer Bedürfnisse weiterzuentwickeln.

Die Konvergenz von IT und OT führt dazu, dass herkömmliche Best Practices, die eine Trennung von IT- und OT-Netzwerken vorsehen, nur noch schwer umsetzbar und nicht mehr zu halten sind. In Deutschland sind die IT- und OT-Systeme großer Wasserbetreiber in der Regel vollständig physisch getrennt und die aktuelle Debatte konzentriert sich darauf, die Vor- und Nachteile beider Ansätze für die Sicherheit herauszustellen. Auch wenn einige wenige Vorreiter das Potenzial von vernetzten ICS und Cloud Computing nutzen (siehe z. B. EGLV in Essen, das Leitsysteme auf einer zentralisierten, virtualisierten Plattform einsetzt und die notwendigen organisatorischen Voraussetzungen geschaffen hat, indem es das Management von IT und OT in eine gemeinsame Abteilungseinheit integriert hat (Mülbaier 2021)), bleiben die meisten Betreiber zurückhaltend. Künftige Forschungsarbeiten sollten sich

die Erfahrungen auf nationaler und internationaler Ebene zunutze machen, um die Debatte mit soliden Beweisen und greifbaren Fakten zu untermauern. Wie in unseren Interviews hervorgehoben wurde, ist ein besseres Verständnis dieser Konvergenz eine zentrale Herausforderung, um 1) ihren Mehrwert in Form von neuen Sicherheitsfunktionen und Vorteilen für den Betrieb der Infrastruktur und 2) die neuen Risiken, die durch die zunehmende Konnektivität entstehen, aufzuzeigen. Diese Herausforderung scheint ein wichtiger Meilenstein zu sein, um das Entstehen einer gemeinsamen Vision unter den deutschen Betreibern zu erleichtern, die Zusammenarbeit zu fördern und die Umsetzung einer klaren Agenda zur Planung der zukünftigen Entwicklung von OT-Systemen zu beschleunigen.

#6 Unterstützung der Verlagerung von ICS von Einzelsystemen zu Cloud-basierten Umgebungen (Link zum Trend: Cloud-Migration)

- Was sind die wichtigsten Anforderungen an ein Cloud-basiertes ICS?
- Wie lassen sich Cloud-basierte ICS effizient schützen?

Es wird erwartet, dass der Wassersektor weitgehend von den Vorteilen von Cloud-Plattformen profitieren wird; es ist jedoch unausweichlich, dass Sicherheitsbrüche enorme Schäden verursachen und die Qualität der Dienstleistung dauerhaft gefährden können. Mit der Nutzung von Cloud-Diensten geben die Betreiber kritischer Infrastrukturen immer einen Teil der Souveränität und Kontrolle ab (UP-KRITIS 2020). Ein vielversprechendes Forschungsfeld ist in diesem Zusammenhang die Entwicklung sicherer Cloud-basierter ICS (manchmal auch als SaaS für ICS - ICSaaS - bezeichnet), die die Verlagerung von ICS von Stand-alone-Systemen zu Cloud-basierten Umgebungen unterstützen (Bhamare et al. 2020). Neben der Entwicklung neuer sicherer kommerzieller Lösungen, die auf die Anforderungen kritischer Infrastrukturen zugeschnitten sind (siehe aktuelle Angebote wie Zero Trust von Microsoft, CIRRUS von Indigy, Industrial Immune System von Darktrace), muss die Forschung die Entwicklung von Lösungen zum Schutz von OT-Infrastrukturen beschleunigen. Dies beinhaltet die Erforschung neuer Systeme zur Erkennung von Eindringlingen in ICS-Systeme auf der Prozesssteuerungsebene (Bhamare et al. 2020), die Entwicklung kryptografiebasierter Lösungen zum Schutz von SCADA-Protokollen und -Kommunikation (Shahzad et al. 2014) oder neuer Sicherheitsmodelle zur Gewährleistung der Integrität von ICS-Daten (z. B. RiskBuster von Cerullo et al. 2016). Ganz allgemein ist die Frage der Sicherheitsrisiken bei der Fernsteuerung von Anlagen im Wassersektor weitgehend ungelöst (BSI 2015) und muss mit einer wissenschaftlichen Risikobewertung im Lichte der derzeit verfügbaren Technologie angegangen werden.

#7 Experimentieren mit Testumgebungen und Simulationsumgebungen (Link zum Trend: Cloud-Migration)

- Wie lassen sich die Risikodimensionen in einem sicheren Umfeld erforschen?
- Welche neuen Methoden gibt es, um die Wechselwirkungen zwischen digitaler und physischer Ebene zu untersuchen?

Um künftige Konfigurationen von ICS in einer sicheren Umgebung zu untersuchen, setzen Forscher:innen auf Prüfstände und Simulationsumgebungen, um die Funktionsweise und die Merkmale realer ICS-Systeme zu reproduzieren (einen detaillierten Überblick über bestehende Testbeds und Simulationsplattformen im Wassersektor finden Sie in Tuptuk et al. 2019). In Singapur wurde das SWaT-Testbed als modernes ICS mit einem sechsstufigen Wasseraufbereitungsprozess konzipiert, der von lokalen SPS autonom gesteuert wird. Es wird eingesetzt, um die Auswirkungen von Cyber- und physischen Angriffen auf das Wasseraufbereitungssystem zu verstehen und die Wirksamkeit von Präventions- und Erkennungsmaßnahmen wie Algorithmen zur Angriffserkennung oder IDS zu bewerten (Mathur et al. 2016). Das WADI-Testbed wurde als Erweiterung von SWaT installiert und um neue Elemente wie Vorratstanks, Verbrauchertanks und Chemikaliendosiersysteme ergänzt (Ahmed et al. 2017). Auf holistische Weise schafft es die DHALSIM digital Twin Open-Source Plattform physikalische Verfahren, Kontrollprozesse und Netzwerkkommunikationen zu simulieren. Somit können Cybersicherheitsexpert:innen ein breites Spektrum an möglichen Netzwerkkonfigurationen modellieren und Cybersicherheitsangriffe durchführen sowie umfangreiche Informationen zur Reaktion der physischen- und der SCADA-Systeme sowie zur Lage der ICS-Komponenten erheben (Murillo et al. 2020).

Neben cyber-physikalischen Testumgebungen ist ein weiteres vielversprechendes Experimentierfeld

die Schaffung neuer virtueller Umgebungen, um die Komplexität von Cyberangriffen und deren Folgen zu untersuchen. Die RISKNOUGHT-Plattform beispielsweise ist eine cyber-physische Stresstest-Plattform, die Wassernetze, den Informationsfluss der Cyber-Ebene und die Rückkopplungen mit den kontrollierten physischen Prozessen modellieren kann (Nikolopoulos et al. 2020). RISKNOUGHT nutzt die Software EPANET für die Simulation physikalischer Prozesse im Wassernetz und ein Netzwerkmodell für das SCADA-System (einschließlich Sensoren und SPS), das in der Lage ist, komplexe Steuerungslogikschemata innerhalb der Simulation zu implementieren. Diese Arten von Plattformen können Wasserbetreibern dabei helfen, die Risikolandschaft besser zu verstehen und Szenarien für die laufende Umgestaltung der digitalen und physischen Infrastruktur zu untersuchen.

Da sich die meisten Studien auf Trinkwassersysteme konzentrieren, könnten künftige Arbeiten auch andere Teile des Wasserkreislaufs einbeziehen, z. B. Abwassernetzte, Bewässerungspraktiken oder die Wasserwiederverwendung. Insbesondere eine kürzlich von Alpha Strike durchgeführte Studie unterstrich die Anfälligkeit von Entwässerungsinfrastrukturen und die potenziellen Auswirkungen komplexer Angriffe, die zu einem mehrwöchigen Zusammenbruch der Abwasserversorgung führen könnten (Heise 2020).

#8 Entwicklung sicherer Lösungen, die die Dezentralisierung der Infrastruktur begleiten (Link zum Trend: Transformation der Infrastruktur)

- Welcher Grad des Monitorings und der Kontrolle ist für ein nachhaltiges Management von dezentralisierten Infrastrukturen und konventionellen Systemen angemessen?
- Wie können Zuverlässigkeit und Sicherheit von zukünftigen Kontrollsystemen hybrider Infrastrukturen vor dem Hintergrund der neuen Zuständigkeitsverteilung zwischen öffentlichen Wasserversorgern, Grundstückseigentümer:innen und weiteren Stakeholdern gesichert werden?
- Wie geht man mit den neuen Schwachstellen um, die durch die Dezentralisierung der Infrastruktur und der Governance-Formen entstehen?

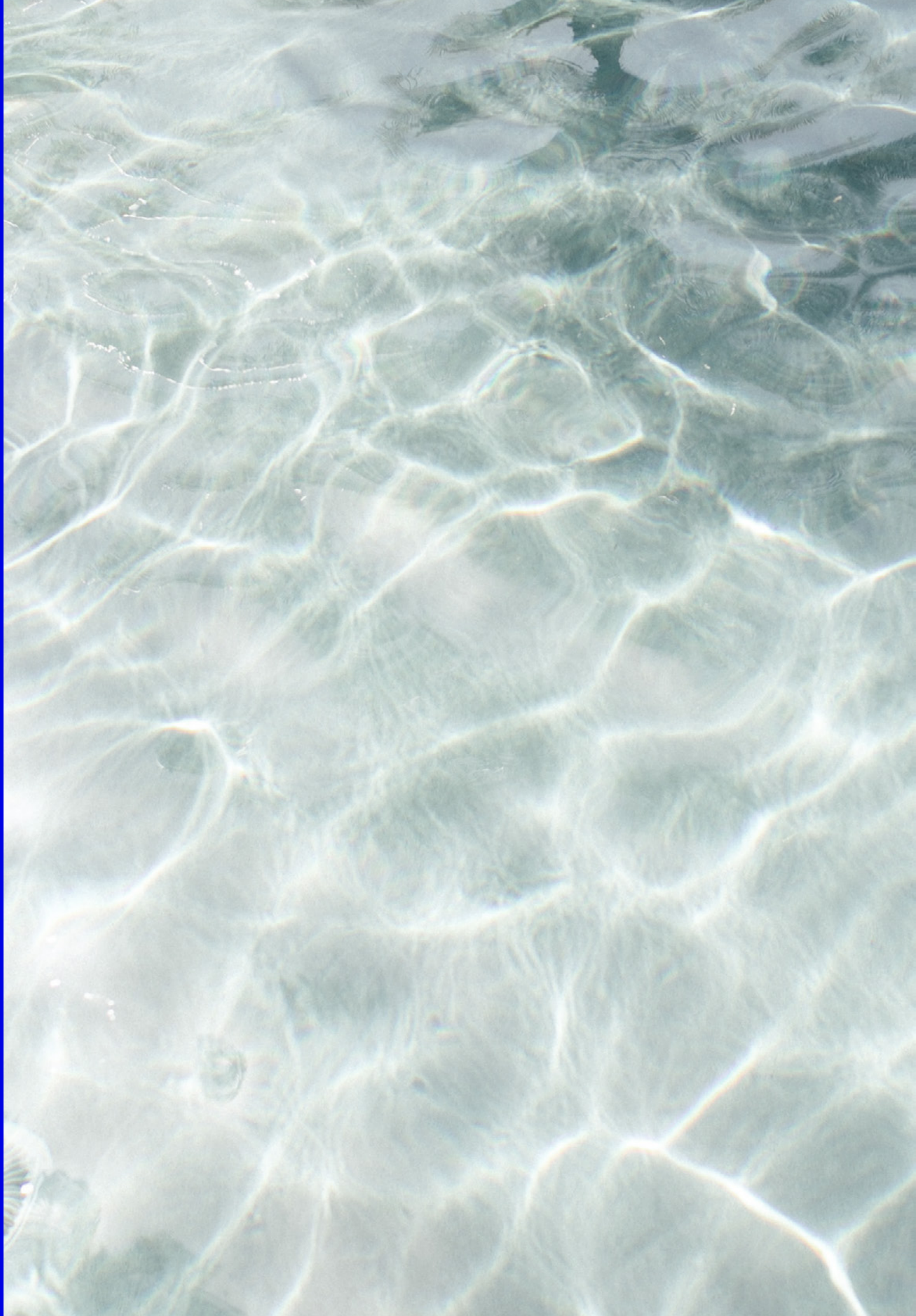
Eine zentrale Herausforderung wird darin bestehen, sichere Lösungen zu finden, um die Transformation der Infrastruktur zu begleiten; insbesondere die Einführung grüner Infrastruktur und dezentraler Lösungen für die Regenwasserbewirtschaftung. Im Moment gibt es noch Unklarheiten über das angemessene Maß an Integration und Unsicherheiten über die Effizienz und Funktionsweise der neuen hybriden Infrastruktur (UN-Water 2018). Forschung ist notwendig, um unser Wissen über die richtige Planung, den Bau und die Pflege grüner Infrastrukturen zu verbessern (Akther et al. 2018). Es werden neue Ansätze benötigt, um von IoT-Lösungen zu profitieren und die wachsende Komplexität der dezentralen Infrastruktur auf lokaler Ebene zu überwachen. Schließlich wird angewandte Forschung notwendig sein, um das richtige Maß an Kontrolle der hybriden Infrastruktur zu definieren, die aus einer Vielzahl heterogener grüner Infrastrukturen zusammen mit konventionellen Wasser- und Abwassernetzen besteht.

Der Paradigmenwechsel von einem konventionellen technischen System zu einem hybriden System mit neuen städtischen Funktionen und partizipativen Governance-Formen (Dhakal und Chevalier 2016) stellt den Schutz der neuen städtischen Wassernutzungen vor große Herausforderungen. Insbesondere ist Forschung erforderlich, um die potenziellen Auswirkungen von Sicherheitsbrüchen auf die Verwaltung hybrider Infrastrukturen sowie die neuen Arten von Risiken, die für die Bürger:innen entstehen könnten, zu verstehen.

#9 Erstellung einer strukturellen Ontologie für Smart Cities (Link zum Trend: Smart City)

- Wie lässt sich die Einheitlichkeit von Standards für Komponenten und Kommunikation gewährleisten?
- Wie lassen sich sichere Rahmenbedingungen und Plattformen für die Zusammenarbeit und den Datenaustausch schaffen?

Einer der wichtigsten Forschungsbedarfe liegt in der Schaffung eines übergreifenden Datenmodells für Smart Cities, das unter Berücksichtigung der Cybersicherheit aufgebaut ist. Abgesehen von der Notwendigkeit, sich von der Produktion projektbasierter Einzellösungen zu distanzieren, die sich nicht in eine übergeordnete Datenstruktur einbetten lassen und dadurch zu Ineffizienzen bei der Erfassung von Best Practices und transversalen Datenerkenntnissen führen, ist es von entscheidender Bedeutung, die gleichen Fallstricke bei der



Festlegung von Standards zu vermeiden (Howell et al. 2017). Da Datenstandards ihrerseits in Bezug auf Umfang oder Format heterogen sein und unter einer mangelnden Akzeptanz leiden können, was zu einer fragmentierten Datenlandschaft beiträgt, ist es notwendig, Smart-City-Ontologien zu entwickeln. Diese Art von Ansatz wird von großen europäischen Initiativen wie Gaia-X oder FIWARE unterstützt, um einheitliche und interoperable intelligente Lösungen zu fördern. Es muss erforscht werden, wie diese neuen globalen Kommunikationsprotokolle so gesichert werden können, dass die Ausweitung der städtischen Datenplattformen nicht eingeschränkt wird, und zwar sowohl in Bezug auf den Umfang als auch auf die Komplexität. Die Cybersicherheit muss in der künftigen Forschung sorgfältig berücksichtigt werden. Es gibt bereits Beispiele für Smart-City-Datenplattformen, wie etwa SMARTIE, die ausdrücklich darauf abzielen (Bohli, Skarmeta et al. 2015, Khan et al. 2017).

#10 Verbesserung der Sicherheit von städtischen Datenplattformen (Link zum Trend: Smart City)

- Wie kann die Datenintegrität und -sicherheit von städtischen Datenplattformen gewährleistet werden?

Städtische Datenplattformen bilden die Grundlage für jede erfolgreiche Smart-City-Strategie. Durch die gemeinsame Nutzung von Daten können neue Synergien und Anwendungen geschaffen und die Governance gestärkt werden. Solche Initiativen werden bereits in mehreren europäischen Städten eingesetzt (siehe z. B. die Erfahrungen der Stadt Paderborn (Digitale Heimat Paderborn 2019)) und dürften mit der Zeit immer größer werden. Neben den rechtlichen und organisatorischen Herausforderungen, die städtische Datenplattformen bewältigen müssen (Hasbini et al. 2018, Ismagilova et al. 2020), müssen sie sich auch mit den unzähligen Bedrohungen der Cybersicherheit auseinandersetzen, denen sie ausgesetzt sind. Insbesondere in dieser Hinsicht ist weitere Forschung zu sicheren und widerstandsfähigen Infrastrukturen für die Datenspeicherung, -verwaltung und -übertragung für solch vielfältige und zugängliche Datensätze erforderlich, um Datendiebstahl oder -manipulation zu verhindern (Stewart et al. 2018). Ein übergreifendes Beispiel ist SSServProv, ein Rahmenwerk, das die Datensicherheit und den Datenschutz in Smart City-Plattformen in einer mehrschichtigen und daher flexiblen Architektur behandelt. Es konzentriert sich auf die End-to-End-Sicherheit und den Datenschutz, so dass die Legitimität und Sicherheit von Dienstanbietern sowie der Schutz der Daten der Bürger:innen gewährleistet sind (Khan et al. 2017). In ähnlicher Weise schlugen Shen et al. (2017) einen Rahmen für die gemeinsame Nutzung städtischer Daten vor, der die Cloud-Infrastruktur der Plattform durch attributbasierte Verschlüsselung schützt und gleichzeitig dynamische Vorgänge unterstützt.

#11 Vermeidung von Kaskadeneffekten und Entwicklung von Strategien zur Schadensbegrenzung (Link zum Trend: Smart City)

- Wie lassen sich die Interdependenzen und Risiken der Smart City identifizieren und visualisieren?
- Wie kann man sich auf Kaskadeneffekte zwischen Betreibern vorbereiten und damit umgehen?
- Wie lässt sich die schnelle Wiederherstellung des Systems im Falle eines Sicherheitsbruchs gewährleisten?
- Auf welche Weise kann man im Fall eines Angriffs effizient reagieren und wie kann man reaktive Maßnahmen im Notfall priorisieren?

Eine der Hauptgefahren im Zusammenhang mit der Vernetzung der Smart City sind Kaskadeneffekte. Störungen in einem Bereich des Netzes eines Betreibers können sich auf das gesamte System auswirken und dazu führen, dass ganze Stadtteile lahmgelegt werden. Dies ist ein zentrales Anliegen, das sowohl auf technischer als auch auf organisatorischer Ebene weiter erforscht werden muss. Maßnahmen zur Identifizierung und Visualisierung von Interdependenzen sowie der Möglichkeit und des Ausmaßes von Kaskadeneffekten in einer Smart-City-Umgebung müssen weiter entwickelt werden (Braun et al. 2018), da sich die meisten Forschungsarbeiten auf diesem Gebiet bisher nur auf einzelne kritische Infrastrukturen konzentriert haben (z. B. Energieinfrastruktur (Tu et al. 2020), Katastrophenmanagement (Rajarajan 2021) und Wasserinfrastruktur (Palleti et al. 2021)). Es ist wichtig, redundante und widerstandsfähige Systeme zu entwickeln, um das Auftreten von Kaskadeneffekten im Falle eines Sicherheitsbruchs zu verhindern (Beck 2017). Um kaskadierende Ausfälle abzumildern ist es jedoch ebenso notwendig, sichere Organisationsstrukturen zu erforschen, die die Zusammenarbeit und den Informationsaustausch zwischen den Betei-

ligten fördern. Dies betrifft auch spezifische Informationsmanagementsysteme, damit die Beteiligten genau wissen, wie sich Angriffe im Netzwerk ausbreiten (Braun et al. 2018). Eine solche Initiative findet sich in Berlin, wo das Projekt Plan B darauf abzielt, gemeinsam neue Sicherheitsmaßnahmen und -strategien zu entwickeln, um die kontinuierliche Kommunikation und den Betrieb im Falle eines Stromausfalls zu gewährleisten (Senatsverwaltung für Inneres 2021). Organisatorische Maßnahmen wie sorgfältig ausgearbeitete Reaktions- und Wiederherstellungspläne werden für den Schutz der Integrität der Smart City von entscheidender Bedeutung sein.

#12 Entwicklung flexibler Cybersicherheitskonzepte für kleine und mittelgroße Betreiber

- Wie können Rahmenbedingungen und Lösungen für die Cybersicherheit an die Bedürfnisse und Besonderheiten kleiner und mittlerer Betreiber angepasst werden?

Nach der BSI-Kritisverordnung gelten Trinkwasserbetreiber als kritische Infrastrukturen, wenn sie mehr als 22 Millionen Kubikmeter Wasser pro Jahr aufbereiten. Abwasserversorger gelten als kritische Infrastrukturen, wenn mehr als 500 000 Einwohner:innen an die Kläranlagen angeschlossen sind. Seit 2018 müssen Betreiber, die als kritische Infrastrukturen gelten, die Anforderungen des Branchenspezifischen Sicherheitsstandards Wasser/Abwasser (kurz: B3S WA) erfüllen, wie z. B. die Einführung eines Informationssicherheitsmanagementsystems und die Meldung relevanter Vorfälle mit Auswirkungen auf die IT-Sicherheit an das Bundesamt für Sicherheit in der Informationstechnik (BSI) (DWA-M 1060). Da sich die aktuelle Verordnung nur auf große Betreiber konzentriert, muss nur ein kleiner Teil des Wassersektors die Anforderungen erfüllen und nachweisen, dass Maßnahmen nach dem Stand der Technik zur Gewährleistung der Cybersicherheit getroffen wurden (Zimmerman 2021). Unseren Gesprächen zufolge dürfte sich diese Verordnung in Zukunft ändern, da der Schwellenwert für die Definition kritischer Infrastrukturen gesenkt werden könnte, um einen ausreichenden Schutz kleiner und mittelgroßer Betreiber zu gewährleisten. Die jüngste Aktualisierung des B3S WA im Jahr 2021 beinhaltet bereits eine breitere Definition von Anlagenkategorien, einschließlich Staudämmen, die für die Entnahme, Speicherung oder Bewirtschaftung von Oberflächenwasser genutzt werden (Marquardt 2021).

Eine zentrale Herausforderung für die Zukunft wird darin bestehen, Cybersicherheitsstandards für kleinere Betreiber zu erreichen, da nicht genügend finanzielle und personelle Ressourcen zur Verfügung stehen, um das erforderliche Wissen innerhalb der Organisation aufzubauen oder zu erhalten (BSI 2017). Auch kleinere Betreiber werden sich dem digitalen Wandel stellen und haben eine Verantwortung gegenüber ihren Kunden, den Schutz der Wasser- und Abwasserinfrastrukturen zu gewährleisten. Forschung und Innovation sind erforderlich, um die Umsetzung von Cybersicherheitsrahmen und -lösungen für kleinere Betreiber zu erleichtern und dabei künftige Entwicklungen der Vorschriften und die zunehmende Verknüpfung von IT- und OT-Systemen in kleineren Netzen zu antizipieren.

#13 Verstärkung der lokalen, regionalen und internationalen Zusammenarbeit im Wassersektor

- Wie kann man Kooperationsmodelle befähigen, um Wissenstransfer über die Sektoren der kritischen Infrastruktur hinweg sowie innerhalb des Wassersektors zu erreichen?

Um die Cybersicherheit in kritischen Infrastrukturen zu fördern, müssen neue Wege der Zusammenarbeit geschaffen werden, um sichere Plattformen für den Informationsaustausch zu bieten und die Entwicklung neuer Best Practices zu fördern. Diese Kooperationsmodelle haben unterschiedliche Größenordnungen: Sie können von der internationalen (z. B. ENISA) und nationalen (z. B. Bundes Security Operations Center) bis zur lokalen Ebene (z. B. CERT) reichen und sektorspezifisch (CERT@Water) oder sektorübergreifend (UP-KRITIS) sein. Da zur Bekämpfung von Cyber-Bedrohungen eine Fülle von organisatorischen und informationellen Ressourcen erforderlich ist, hat die Entwicklung weiterer Modelle für die (inter-) sektorale Zusammenarbeit, insbesondere bei kritischen Infrastrukturen, höchste Priorität. Diese Einrichtungen müssen dynamisch und eng mit den Versorgungsdienstleistern verbunden sein, um kontinuierlich zeitnahe und effektive Sicherheitsanalysen und sicherheitspolitische Empfehlungen zu gewährleisten (Bhatt et al. 2014).

In NRW beispielsweise wird derzeit auf Initiative von KDW, lokalen Betreibern, DWA und DVGW eine neue Initiative mit dem Namen CERT@Water entwickelt. Sie zielt darauf ab, die Ressourcen der Wasserbetreiber zu bündeln, um das Fachwissen und die Reaktionsfähigkeit des Sektors zu erhöhen.

Sie soll insbesondere die lokalen Wasserbetreiber bei der Überwachung und Klassifizierung von Bedrohungen unterstützen und Maßnahmen zur Verbesserung der Vorbeugung, Reaktion und Sensibilisierung innerhalb der Organisationen einleiten. Das Hauptziel der Gruppe ist die Bündelung des Fachwissens in einer zentralen Einrichtung auf regionaler Ebene, die allen lokalen Betreibern, insbesondere kleinen und mittleren, Beratung, Empfehlungen und Fachwissen bieten kann.

Auf nationaler Ebene dient UP-KRITIS als zentraler Helpdesk, der über neue und laufende Cyber-Bedrohungen informiert (UP KRITIS 2014). Die Mitglieder des UP KRITIS arbeiten in sektorspezifischen und sektorübergreifenden Gremien zu technischen und organisatorischen Fragen im Zusammenhang mit dem Schutz kritischer Infrastrukturen zusammen. Die Mitglieder tauschen sich aus und lernen voneinander zu Themen wie der aktuellen Bedrohungslage, dem Stand der Technik oder Verfahren zum Krisenmanagement. Durch die Weiterentwicklung der Kompetenzen solcher Institutionen wird ein Kreislauf in Gang gesetzt, dem weitere Versorgungsdienstleister beitreten wollen, was wiederum den Umfang und die Tiefe der Dienstleistungen weiter verbessert (Clemente 2018).

Schließlich wurde im Oktober 2021 nach Abschluss des europäischen Projekts STOP-IT (STOP-IT 2021) der Prozess zur Schaffung eines europäischen Water Information Sharing & Analysis Center (ISAC) in noch größerem Umfang eingeleitet. Dies geschah auch vor dem Hintergrund, dass die Europäische Kommission zusammen mit ENISA, der Agentur der Europäischen Union für Cybersicherheit, die in Zusammenarbeit mit CERT-EU regelmäßig Best Practices für die Cybersicherheit veröffentlicht, einen Auftrag an kritische Infrastrukturen erteilte, eigene ISACs zu entwickeln (Capgemini 2020). Das European WaterISAC ist daher ein Paradebeispiel für die künftige Entwicklung der Cybersicherheits-Zusammenarbeit zwischen Wasserversorgern und sollte als Leitlinie für den Forschungsbedarf in diesem Sektor dienen.

#14 Entwicklung neuer und verbesserter Bildungs- und Ausbildungsprogramme und Erhöhung der Attraktivität des Sektors für IT- und OT-Expert:innen

- Wie kann menschliches Versagen in der Cybersicherheit reduziert werden?
- Wie kann das Bewusstsein der Mitarbeiter:innen für die Cybersicherheit auf der Ebene des Top-Managements, in den IT-OT-Abteilungen und allgemein auf Unternehmensebene geschärft werden?
- Wie kann dem Fachkräftemängel des Wasser- und IT-Sektors entgegengewirkt werden?

Menschliches Versagen wird im Allgemeinen als einer der wichtigsten Faktoren für Verletzungen der Cybersicherheit angesehen. Der menschliche Faktor spielt bei der Mehrheit der Cybersicherheitsvorfälle eine Schlüsselrolle, einschließlich Fehlerquellen wie mangelhafte Software-Patches oder unzureichende Kommunikation im Zusammenhang mit sensiblen Informationen (Nobles 2018). Ein aktueller Bericht von IBM fand heraus, dass 23 % der Datenschutzverletzungen direkt durch menschliches Versagen verursacht werden (IBM 2021). Da ein Großteil der Verstöße gegen die Cybersicherheit auf menschliches Versagen zurückzuführen ist, insbesondere angesichts der jüngsten und weit verbreiteten Zunahme von Phishing- und Social-Engineering-Angriffen (Interview), ist es von entscheidender Bedeutung, Best Practices zu erforschen und zu entwickeln, mit denen die Cybersicherheitskenntnisse und -kompetenzen der Mitarbeiter:innen auf allen Ebenen des Unternehmens gefördert werden können (Slaughter et al. 2017).

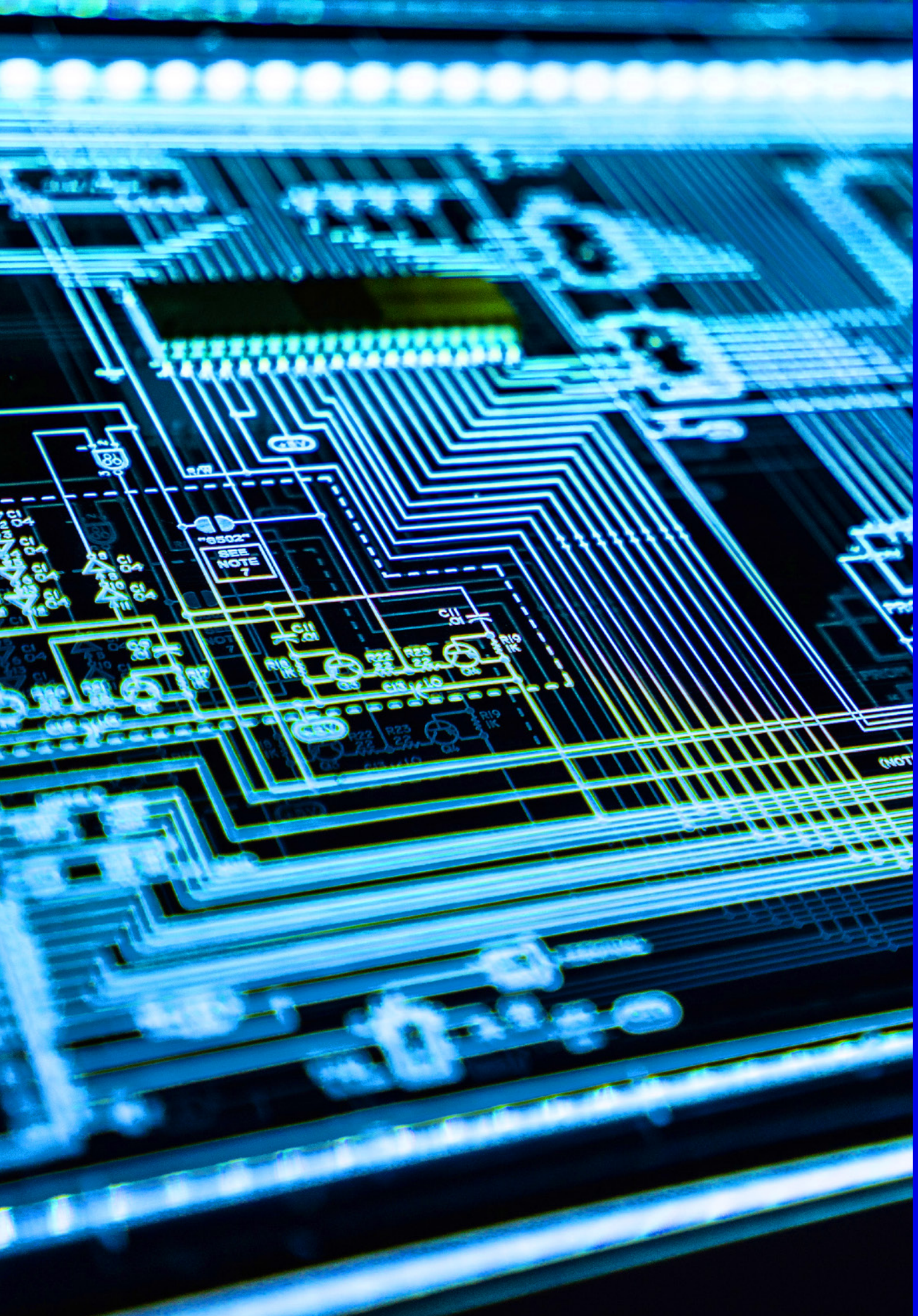
Im Bereich der Aus- und Weiterbildung gibt es mehrere Ansatzpunkte für weitere Forschung und Entwicklung. Erstens müssen für die Wasserinfrastruktur spezifische Maßnahmen entwickelt werden, mit denen die Cybersicherheitsreife (z. B. ES-C2M2 für Energie und ONG-C2M2 für Öl und Gas (Curtis und Mehravari 2015)) und die Cybersicherheitskompetenz der Mitarbeiter:innen (z. B. Human Aspects of Information Security Questionnaire (Parsons et al. 2014)) bewertet werden können.

Der zweite Forschungsbereich besteht darin, die idealen Ansätze für Cybersicherheitstrainings für kritische Infrastrukturen zu verstehen, was durch Chowdhury und Gkioulos (2021), die vor allem die Energieinfrastruktur analysierten, erheblich gefördert wurde. Dabei kamen sie zu dem Schluss, dass sich

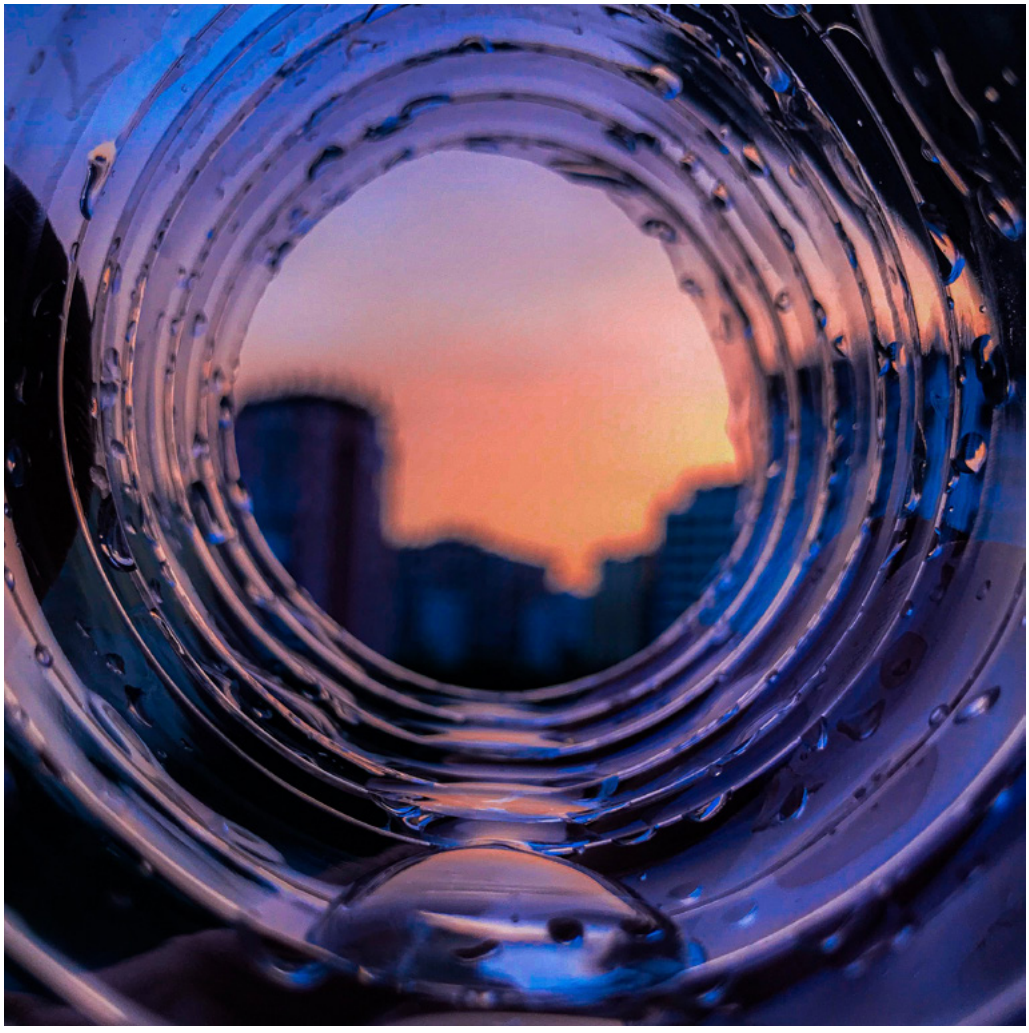
praxisnahe, interaktive und in die tägliche Routine integrierte Aus- und Weiterbildungsprogramme als am wirksamsten für die Verbesserung der Cybersicherheitskompetenz erweisen. Daher sollten solche Ansätze im Mittelpunkt der künftigen Forschung stehen. Im Rahmen der interaktiven Ansätze lassen sich schließlich drei übergreifende Methoden für die Aus- und Weiterbildung ausmachen: Die spielbasierte Ausbildung kann aus Videospielen (z. B. CyberCIEGE (Cone et al. 2007)), Serious Games (z. B. AWT.103 Zero Downtime: Blackout Edition (LIMES Security 2021) oder TORC aus dem STOP-IT-Projekt) und Rollenspielen bestehen (z. B. SWaT Security Showdown (Antonioli et al. 2017)). Und die Trainingsmethoden können simulationsbasiert (z. B. SECPSIM (Vellaithurai et al. 2013) oder CLAAS (Tunc et al. 2015)) oder Testbed-basiert sein (z. B. Hybrid Testbeds for Critical Infrastructures (Leps 2018) oder ISAAC (Oyewumi et al. 2019)).

Da ein großer Teil der diesbezüglichen Forschung im Kontext des Energiesektors durchgeführt wurde, besteht ein erheblicher Bedarf an weiterer Forschung und Entwicklung solcher Maßnahmen, die auf Wasserbetreiber zugeschnitten sind.

Zusätzlich zur Stärkung betriebsinterner Kompetenzen müssen auch Ansätze erforscht werden, um eine neue Generation von OT-, IT- und Cybersicherheitsexpert:innen auszubilden, die den neuartigen Herausforderungen des Wasser 4.0 gewachsen sind. Gleichzeitig muss die Attraktivität dieser Karrieren, sowie solcher im Wassersektor im Allgemeinen gesteigert werden, um dem sich stetig verschärfenden Fachkräftemangel entgegenzusteuern. Auch hier hatte die Covid-19-Pandemie einen erheblichen Einfluss, da die Einwanderung ausgebildeter Fachkräfte deutlich zurückging. Neben veralteten Ausbildungsformaten und -inhalten für angehende OT-Expert:innen bilden auch die mit anderen Sektoren vergleichsweise niedrigen Gehälter für IT-Expert:innen große Hürden auf dem Weg zum Wasser 4.0. In einem Bericht des Bundesministeriums für wirtschaftliche Zusammenarbeit und Entwicklung zur beruflichen Bildung im Wassersektor (BMZ 2016) werden einige Handlungsempfehlungen formuliert, die sich angesichts der aktuellen Arbeitnehmer:innenknappheit auch auf Deutschland übertragen lassen. Besonders die darin erwähnte Wechselwirkung zwischen ansteigenden Qualifikationsanforderungen im Wassersektor und gleichzeitiger Abwanderung in die besser zahlende Privatwirtschaft sobald diese Qualifikationen vorliegen, lässt sich im inländischen Kontext wiederfinden, besonders im IT- und Cybersicherheitsbereich. Es lässt sich also ein zentraler Handlungsbedarf in der Schaffung von Anreizsystemen, die den Verbleib im Wassersektor attraktiv machen, verzeichnen. Bezüglich der Ausbildung wird in diesem Bericht die Effektivität des dualen Berufsbildungssystems festgehalten, auch dieses sollte im inländischen Kontext stärker gewichtet und weiter ausgebaut werden, um den deutschen Wassersektor mit neuen OT- und IT-Expert:innen zu bereichern.


"6502"
SEE
NOTE
7

Fazit und Ausblick



Die Wasserinfrastruktur steht einem enormen Wandel bevor. Um die aktuellen globalen Herausforderungen des Klimawandels und des enormen Bevölkerungswachstums zukünftig begegnen zu können, muss eine umfassende Modernisierung und Digitalisierung der Infrastrukturen und Praktiken der Siedlungswasserwirtschaft erfolgen.

Das Wasser 4.0 führt zu einer klaren Erhöhung der Effizienz und Nachhaltigkeit gegenüber der herkömmlichen Wasserinfrastruktur, sei es durch Prozessinnovationen, der Schaffung neuer Anwendungen oder der Stärkung transversaler Synergieeffekte. Diese Entwicklungen können jeweils als Fortschritte in der Datenerhebung und -auswertung, in der informationellen und operationellen Infrastruktur und in der Interoperabilität und Zusammenarbeit klassifiziert werden. Somit haben sich fünf Entwicklungsschwerpunkte kristallisiert (IoT und Intelligente Sensoren, KI für die Wasserwirtschaft, Cloud-Migration, Transformation der Infrastruktur und Smart Cities), die neben ihren enormen Potenzialen jedoch auch beachtliche Gefahren bergen.

Um ein optimal funktionierendes urbanes Wassermanagement zu gewährleisten, bedarf es eines drastischen Ausbaus der Cybersicherheit, sowohl in technischer als auch personeller Hinsicht. Die Lage der Cybersicherheit des deutschen Wassersektors wurde vom KDW als „kritisch“ eingestuft (KDW 2021) und die Bewältigung dieser neuartigen Herausforderung ist aufgrund mehrerer Faktoren, wie fehlende Infrastrukturen, Ressourcen und besonders Kompetenzen und Fachkräfte, deutlich erschwert. Deswegen wurden in diesem Bericht vor allem die Cyberrisiken, die mit den Entwicklungsschwerpunkten einhergehen sowie erste vielversprechende Ansätze diese zu bewältigen, durchleuchtet, um zur Gestaltung einer sicheren und innovativen Zukunftslandschaft der Wasserwirtschaft beizutragen. Dabei wurden die folgenden Forschungs- und Entwicklungsbedarfe identifiziert:

- Verbesserung der Sicherheit von IoT-Komponenten
- Aufbau von KI-basierten fortschrittlichen Analysen für Cybersicherheitsprobleme
- Erfassung des realen Verhaltens von Analyst:innen bei der Entwicklung von KI-Algorithmen
- Reduzierung der Einschränkungen von KI und Erhöhung der Robustheit von Vorhersagen
- Verbesserung des Verständnisses für neue Sicherheitsprobleme im Zusammenhang mit der Konvergenz von IT- und OT-Systemen
- Unterstützung der Verlagerung von ICS von eigenständigen Systemen zu Cloud-basierten Umgebungen
- Experimentieren mit Testbeds und Simulationsumgebungen
- Entwicklung sicherer Lösungen, die die Dezentralisierung der Infrastruktur begleiten
- Erstellung einer strukturellen Ontologie für Smart Cities
- Verbesserung der Sicherheit von städtischen Datenplattformen
- Vermeidung von Kaskadeneffekten und Entwicklung von Abhilfestrategien
- Entwicklung flexibler Cybersicherheitsansätze für kleine und mittelgroße Betreiber
- Verstärkung der lokalen, regionalen und internationalen Zusammenarbeit im Wassersektor
- Entwicklung neuer und verbesserter Ausbildungs- und Schulungsprogramme und Erhöhung der Attraktivität des Sektors für IT- und OT-Expert:innen

Anhand dieser Handlungsbedarfe kann ein Weg hin zu widerstandsfähigeren und cyber-sicheren Wasserinfrastrukturen gebahnt und somit die Sicherheit und Gesundheit von Mensch und Umwelt gewährleistet werden.

Referenzen

#

120 Water (2021) Abgerufen von https://120water.com/preparing-for-the-water-industrys-retirement-wave/ (01.06.2022).

A

ACALVIO (2022) Abgerufen von https://www.acalvio.com/ (01.06.2022).

Adelmeyer, M. und F. Teuteberg (2018) Cloud Computing Adoption in Critical Infrastructures-Status Quo and Elements of a Research Agenda. Proceedings of the Multikonferenz Wirtschaftsinformatik 2018: 1345-1356.

Adu-Manu, K. S., et al. (2017) Water quality monitoring using wireless sensor networks: Current trends and future research directions. ACM Transactions on Sensor Networks (TOSN) 13(1): 1-41.

Ahmed, A. N., et al. (2019) Machine learning methods for better water quality prediction. Journal of Hydrology 578: 124084.

Ahmed, C. M., Palleti, V. R., & Mathur, A. P. (2017) WADI: a water distribution testbed for research in the design of secure cyber physical systems. In Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks (pp. 25-28).

Aich, A. und A. Sen (2015) Study on cloud security risk and remedy. Int. J. Grid Distrib. Comput 8(2): 155-166.

Akther, M., He, J., Chu, A., Huang, J., van Duin, B. (2018) A review of green roof applications for managing urban stormwater in diferent climatic zones. Sustainability, 10. Abgerufen von https://doi.org/10.3390/su10082864 (01.06.2022).

Alam, M. P. und D. Manoharan (2016) Design and Development of Autonomous Amphibious Unmanned Aerial Vehicle and UAV Mountable Water Sampling Devices for Water Based Applications, SAE Technical Paper.

Alghofaili, Y., et al. (2021) Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. Applied Sciences 11(19): 9005.

Almeida, F., et al. (2020) The challenges and opportunities in the digitalization of companies in a post-COVID-19 World. IEEE Engineering Management Review 48(3): 97-103.

Almiani, M., et al. (2020) Deep recurrent neural network for IoT intrusion detection system. Simulation Modelling Practice and Theory 101: 102031.

Amsterdam Rainproof (2016) "Amsterdam Rainproof." Abgerufen von https://amsterdamsmartcity.com/updates/project/amsterdam-rainproof (01.06.2022).

Amsterdam Rainproof (o. J.) Amsterdam Rainproof G. v. Eijck. Amsterdam.

Anton, S. D. D., et al. (2019) Anomaly-based intrusion detection in industrial data with SVM and random forests. 2019 International conference on software, telecommunications and computer networks (SoftCOM), IEEE.

Antonioli, D., et al. (2017) Gamifying ICS security training and research: Design, implementation, and results of S3. Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy.

Apostu, A., et al. (2014) New classes of applications in the cloud. Evaluating advantages and disadvantages of cloud computing for telemetry applications. Database Systems Journal 5(1): 3-14.

Appian (2019) "Anglian Water." Abgerufen von https://appian.com/why-appian/customers/all-customers/anglian-water.html (01.06.2022).

aqua3s (o. J.) "The project." Abgerufen von https://aqua3s.eu/the-project.

Aquatech (2021) "Capturing new talent to transform water." Abgerufen von https://www.aquatechtrade.com/news/utilities/capturing-talent-to-transform-water/ (01.06.2022) .

ASCE - American Society of Civil Engineers (2020) The Economic Benefits of Investing in Water Infrastructure - How a Failure to Act Would Affect the US Economic Recovery. Value of Water Campaign, American Society of Civil Engineers, ASCE.

ASCE - American Society of Civil Engineers (2021) 2021 Report Card for America's Infrastructure.

Ayala, I., et al. (2015) The Sol agent platform: Enabling group communication and interoperability of self-configuring agents in the Internet of Things. Journal of Ambient Intelligence and Smart Environments 7: 243-269.

B

Baanu, B. B. und K. J. Babu (2021) Smart water grid: a review and a suggestion for water quality monitoring. Water Supply.

Barthelemy, J., et al. (2020) Problem-Driven and Technology-Enabled Solutions for Safer Communities: The case of stormwater management in the Illawarra-Shoalhaven region (NSW, Australia). Handbook of Smart Cities: 1-28.

BBK, B. f. B. u. K.-. (o. J.) "Kritische Infrastrukturen". Abgerufen von https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html (01.06.2022).

Beck, K. (2017) Smart Security?:Evaluating Security Resiliency in the U.S. Department of Transportation's Smart City Challenge. Transportation Research Record 2604(1): 37-43.

Bhamare, D., et al. (2020) Cybersecurity for industrial control systems: A survey. Computers & security 89: 101677.

Bhatt, S., et al. (2014) The Operational Role of Security Information and Event Management Systems. IEEE security & Privacy 12(5): 35-41.

Biggio, B. und F. Roli (2018) Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition 84: 317-331.

Birkett, D.M. (2017) Water Critical Infrastructure Security and Its Dependencies. Journal of Terrorism Research, 8(2), pp.1–21.

BMI, B. d. I. u. f. H.-. (2020) Neue Leipzig Charta.

BMZ (2016) Berufliche Bildung im Wassersektor. B. f. w. Z. u. Entwicklung. Bonn, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

Bock, K., et al. (2018) Sensor Technologien 2022. R. Werthschützky. Berlin, AMA Verband für Sensorik und Messtechnik e.V.

Boyes, H., et al. (2018) The industrial internet of things (IIoT): An analysis framework. Computers in industry 101: 1-12.

Braun, T., et al. (2018) Security and privacy challenges in smart cities. Sustainable Cities and Society 39: 499-507.

Brem, T. (2021) Cybersicherheit im Smart Grid. FMS-BERICHTE: 64.

Bresniker, K., et al. (2019) Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity. IEEE Computer Society.

Brutti, A., et al. (2019) Smart city platform specification: A modular approach to achieve interoperability in smart cities. The internet of things for smart urban ecosystems, Springer: 25-50.

BSI, B. f. S. i. d. I.-. (2015) KRITIS-Sektorstudie - Ernährung und Wasser. B. f. S. i. d. Informationstechnik. Bonn, Bundesamt für Sicherheit in der Informationstechnik.

BSI, B. f. S. i. d. I.-. (2017) BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz. B. f. S. i. d. Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik.

BSI, B. f. S. i. d. I.-. (2020) Die Lage der IT-Sicherheit in Deutschland 2020. B. f. S. i. d. Informationstechnik. Bonn, Bundesamt für Sicherheit in der Informationstechnik.

BSI, B. f. S. i. d. I.-. (2021) Orientierungshilfe zu Inhalten und Anforderungen an branchen-spezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG. B. f. S. i. d. Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik.

BSI, B. f. S. i. d. I.-. (o. J.) "Nachweise gemäß § 8a Absatz 3 BSIG." Abgerufen von https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Nachweise-erbringen/nachweise-erbringen.html (01.06.2022).

Buyya, R., et al. (2018) A manifesto for future generation cloud computing: Research directions for the next decade. ACM computing surveys (CSUR) 51(5): 1-38.

C

Capdevila, A. S. L., et al. (2020) Success factors for citizen science projects in water quality monitoring. Science of the Total Environment 728: 137843.

Capgemini (2020) "EU erteilt Auftrag zum Auf- und Ausbau von Informationsaustausch- und Analysezentren (ISACs)." Abgerufen von https://www.capgemini.com/de-de/news/isac-ausbau-eu-kommission (01.06.2022).

Caradot, N., et al. (2022) Smart water management. Springer Handbook of Internet of Things.

Carlini, N. und D. Wagner (2017) Towards evaluating the robustness of neural networks. 2017 ieee symposium on security and privacy (sp), IEEE.

Cerullo, G., et al. (2016) A Secure Cloud-Based SCADA Application: The Use Case of a Water Supply Network. SoMeT.

Chan, L., et al. (2019) Survey of AI in cybersecurity for information technology management. 2019 IEEE technology & engineering management conference (TEMSCON), IEEE.

Chang, J., et al. (2014) Graphene-based sensors for detection of heavy metals in water: a review. Analytical and bioanalytical chemistry 406(16): 3957-3975.

Chastain-Howley, A. (2018) Smart Water Solutions - BIG DATA BRINGING OPTIMIZATION TO LIFE FOR WATER UTILITIES. Black & Veatch Strategic Directions. B. Veatch, Black & Veatch. WATER REPORT.

Chen, F., et al. (2020) Open water detection in urban environments using high spatial resolution remote sensing imagery. Remote Sensing of Environment 242: 111706.

Chen, Y., et al. (2018) Extraction of urban water bodies from high-resolution remote-sensing imagery using deep learning. Water 10(5): 585.

Cherqui, F., et al. (2019) Toward proactive management of stormwater control measures using low-cost technology. Novatech 2019.

Chowdhury, N. und V. Gkioulos (2021) Cyber security training for critical infrastructure protection: A literature review. Computer Science Review 40: 100361.

Chowdury, M. S. U., et al. (2019) IoT Based Real-time River Water Quality Monitoring System. Procedia Computer Science 155: 161-168.

Chung, W.-C., et al. (2014) CloudDOE: a user-friendly tool for deploying Hadoop clouds and analyzing high-throughput sequencing data with MapReduce. PloS one 9(6): e98146.

City-zen (2019) "A Tale of Two Cities." Abgerufen von http://www.cityzen-smartcity.eu/wp-content/uploads/2019/11/interactive_final-deliverable-book.pdf.

Clark, R. M., et al. (2016) Protecting drinking water utilities from cyberthreats. Journal of the American Water Works Association 109(INL/JOU-16-39302).

Clemente, J. F. (2018) Cyber security for critical energy infrastructure, NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Cloud Security Alliance, C. (2018) Top Threats to Cloud Computing: Deep Dive.

Coles-Kemp, L. und R. R. Hansen (2017) Walking the line: The everyday security ties that bind. International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer.

Compagnucci, L. und F. Spigarelli (2018) Fostering Cross-Sector Collaboration to Promote Innovation in the Water Sector. Sustainability 10(11): 4154.

Cone, B. D., et al. (2007) A video game for cyber security training and awareness. Computers & security 26(1): 63-72.

Conejos Fuertes, P., et al. (2020) Building and exploiting a Digital Twin for the management of drinking water distribution networks. Urban Water Journal 17(8): 704-713.

Cukier, K. (2010) Data, data everywhere: A special report on managing information. The Economist.

Curtis, P. D. und N. Mehravari (2015) Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. 2015 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE.

D

Dembski, F., et al. (2020) Urban digital twins for smart cities and citizens: The case study of Herrenberg, Germany. Sustainability 12(6): 2307.

Derrick, B. E. und M. Moore (2015) An Alternative Approach to Illicit Discharge Detection with Aerial Infrared Thermal Imagery. A Case Study of MS4 Dry Weather Illicit Discharge Screening. Proceedings of the Water Environment Federation 2015(18): 1290-1308.

Dhakal, K. P. und L. R. Chevalier (2015) Implementing low impact development in urban landscapes: A policy perspective. World Environmental and Water Resources Congress 2015.

Dhakal, K. P. und L. R. Chevalier (2016) Urban stormwater governance: the need for a paradigm shift. Environmental management 57(5): 1112-1124.

DHI (o. J.) "MIKE WaterNet Advisor." Abgerufen von https://www.mikepoweredbydhi.com/products/waternet-advisor.

Dickerson, S. T. und A. Butler (2018) Resolve Workforce Challenges to ensure future success at water and wastewater utilities. Opflow 44(9): 8-9.

digital-water.city (2022) "Leading urban water management to its digital future." Abgerufen von https://www.digital-water.city/ (01.06.2022).

Digitale Heimat Paderborn (2019) "Zentrale Open Data Plattform." Abgerufen von https://digitale-heimat-pb.de/projekte/zentrale-open-data-plattform/ (01.06.2022).

Dogo, E. M., et al. (2019) Blockchain and Internet of Things-Based Technologies for Intelligent Water Management System. Artificial Intelligence in IoT. F. Al-Turjman. Cham, Springer International Publishing: 129-150.

Dzombak, D. A., et al. (2012) Sensing for Improved Water Infrastructure Management in 2050. Toward a Sustainable Water Future: Visions for 2050: 253-262.

E

El-Zahab, S. und T. Zayed (2019) Leak detection in water distribution networks: an introductory overview. Smart Water 4(1): 1-23.

ENVIRAIoT (o. J.) "Flood monitoring and warning system." Abgerufen von https://enviraiot.com/flood-monitoring-warning-system/ (01.06.2022).

Eremia, M., et al. (2017) The smart city concept in the 21st century. Procedia Engineering 181: 12-19.

European Commission (2021) Pathway to a Healthy Planet for AllEU Action Plan: 'Towards Zero Pollution for Air, Water and Soil'.

F

Fab Lab Barcelona (o. J.) "Soil and water sensors." Smart Citizen Docs. Abgerufen von https://docs.smartcitizen.me/Components/Soil %20and %20water/ (01.06.2022).

Falliere, N., et al. (2011) Symantec security response: W32. stuxnet dossier. Symantec Corporation, February.

Fiware4Water (o. J.-a) "Links between Fiware and Fiware4Water." Abgerufen von https://www.fiware4water.eu/about/links-between-fiware-and-fiware4water (01.06.2022).

Fiware4Water (o. J.-b) "Project summary." Abgerufen von https://www.fiware4water.eu/about/links-between-fiware-and-fiware4water (01.06.2022).

Fluence (o. J.) "Decentralized Wastewater Treatment." Abgerufen von https://www.fluencecorp.com/decentralized-wastewater-treatment/.

FLUIDION (o. J.) "General Overview." Abgerufen von https://www.fluidion.com/en/products/8-main/17-produits-presentation.

Flyability (2022) "WinCan and Flyability partner on end-to-end solution for wastewater inspection and management." Abgerufen von https://www.flyability.com/news/wincan-partnership (01.06.2022).

Flyability (o. J.) "Inside Barcelona's Sewer System: Drone Inspection Is the Best Response to an Environment Emergency." Abgerufen von https://www.flyability.com/casestudies/inside-barcelonas-sewer-system-drone-inspection-is-the-best-response-to-an-environment-emergency (01.06.2022).

Folkman, S. (2018) Water main break rates in the USA and Canada: A comprehensive study.

Frascella, A., et al. (2018) A minimum set of common principles for enabling Smart City Interoperability. TECHNE-Journal of Technology for Architecture and Environment: 56-61.

G

Gaia-X (2021) Gaia-X Domäne Smart City/ Smart Region.

Galfi, H. (2022) Turbinator - A new turbidity and water level sensor. Gothenburg, City of Gothenburg.

Gandomi, A. und M. Haider (2015) Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management 35(2): 137-144.

Gartner (2021) Gartner Forecasts Worldwide Low-Code Development Technologies Market to Grow 23 % in 2021

Gates Foundation (o. J.) "Reinvent the Toilet Challenge: A brief history." Abgerufen von https://www.gatesfoundation.org/our-work/programs/global-growth-and-opportunity/water-sanitation-and-hygiene/reinvent-the-toilet-challenge-and-expo (01.06.2022).

Gelsenwasser (2020) "Trio kündigt digitalen Trinkwasserzähler für den deutschen Markt an." Abgerufen von https://www.gelsenwasser.de/news-blog/pressemeldungen/kamstrup (01.06.2022).

Georgescu, T.-M., et al. (2019) Named-entity-recognition-based automated system for diagnosing cybersecurity situations in IoT networks. Sensors 19(15): 3380.

Geyler, S., et al. (2019) Sustainable Stormwater Management in Existing Settlements—Municipal Strategies and Current Governance Trends in Germany. Sustainability 11(19): 5510.

Ghaeini, H. R., et al. (2019) Zero residual attacks on industrial control systems and stateful countermeasures. Proceedings of the 14th International Conference on Availability, Reliability and Security.

Gkoumas, K., et al. (2012) Energy Harvesting Applications in Transportation Infrastructure Networks. Procedia - Social and Behavioral Sciences 48: 1097-1107.

Global Water Research Coalition, G. (2021) The Digital Water Utility of the Future.

GlobalData (2019) Smart cities – Thematic Research 51.

Göteborg (2020) The LoV-IoT project: Air and water monitoring with Internet of Things. E. Administration. Göteborg, City of Gothenburg.

GovTech Singapore (2020) "Doubling down on cloud to deliver better government services."

Grant, S. B., et al. (2012) Taking the "waste" out of "wastewater" for human water security and ecosystem sustainability. Science 337(6095): 681-686.

Grieves, M. und J. Vickers (2017) Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. Transdisciplinary perspectives on complex systems, Springer: 85-113.

Guo, G., et al. (2018) Short-Term Water Demand Forecast Based on Deep Learning Method. Journal of Water Resources Planning and Management 144(12): 04018076.

H

Hahn, A. (2016) Operational technology and information technology in industrial control systems. Cyber-security of SCADA and other industrial control systems, Springer: 51-68.

Hall, R., et al. (2000) The vision of a smart city. 2nd Int. Life .

Hamburg (o. J.) " Urbane Daten – ohne sie geht fast nichts mehr! ". Abgerufen von http://www.urbandataplatform.hamburg/was-ist-die-urban-data-platform-hamburg/11696646/was-ist-die-urban-platform/ (01.06.2022).

Hasbini, M. A., et al. (2018) Investigating the information security management role in smart city organisations. World Journal of Entrepreneurship, Management and Sustainable Development.

Hassanzadeh, A., et al. (2020) A review of cybersecurity incidents in the water sector. Journal of Environmental Engineering 146(5): 1-13.

Heise, (2020) Abgerufen von https://www.heise.de/news/Angriffswarnung-Massive-IT-Sicherheitsluecken-in-Berliner-Wasserbetrieben-4858333.html (01.06.2022).

Hoang, L. und R. A. Fenner (2016) System interactions of stormwater management using sustainable urban drainage systems and green infrastructure. Urban Water Journal 13(7): 739-758.

Howell, S., et al. (2017) Integrating building and urban semantics to empower smart water solutions. Automation in Construction 81: 434-448.

Huang, C., et al. (2018) Detecting, extracting, and monitoring surface water from space using optical sensors: A review. Reviews of Geophysics 56(2): 333-360.

I

IBM (2021) Cost of a Data Breach Report 2021. Armonk, IBM Corporation.

ICT4Water (2018) "Action Group Interoperability & Standardization." Abgerufen von http://webcache.googleusercontent.com/search?q=cache:https://ict4water.eu/action-group-interoperability-standardization/ (01.06.2022).

Inductive Automation (2011) Cloud-Based SCADA Systems: The Benefits & Risks.

Ingles, J., et al. (2021) Water quality assessment using a portable UV optical absorbance nitrate sensor with a scintillator and smartphone camera. Water SA 47(1): 135-140.

IPK - Impulse pro Kanal (2020) Inspektion Sanierung Erneuerung

Ismagilova, E., et al. (2020) Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers: 1-22.

Ismail, N., et al. (2019) Smart irrigation system based on internet of things (IOT). Journal of Physics: Conference Series, IOP Publishing.

J

Jagielski, M., et al. (2018) Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. 2018 IEEE Symposium on Security and Privacy (SP).

Jan, F., et al. (2021) Iot based smart water quality monitoring: Recent techniques, trends and challenges for domestic applications. Water 13(13): 1729.

Javed, B., et al. (2017) Internet of things (IoT) design considerations for developers and manufacturers. 2017 IEEE International Conference on Communications Workshops (ICC Workshops).

Jeong, S., et al. (2020) City Data Hub: Implementation of Standard-Based Smart City Data Platform for Interoperability. Sensors 20(23): 7000.

Jo, S., et al. (2015) A Comparative Study on the Performance of Intrusion Detection using Decision Tree and Artificial Neural Network Models. Journal of Korea Society of Digital Industry and Information Management 11(4): 33-45.

K

Kalinin, M., et al. (2021) Cybersecurity Risk Assessment in Smart City Infrastructures. Machines 9(4): 78.

Kaplan, A. und M. Haenlein (2019) Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons 62(1): 15-25.

Karagiannidis, L., et al. (2016) A CPS-enabled architecture for sewer mining systems. 2016 International Workshop on Cyber-physical

Systems for Smart Water Networks (CySWater), IEEE.

KDW, K. D. W.-. (2021) Ist-Situation in der Wasserwirtschaft, Kompetenzzentrum Digitale Wasserwirtschaft - KDW

Kerkez, B., et al. (2016) Smarter Stormwater Systems. Environmental Science & Technology 50(14): 7267-7273.

Khan, Z., et al. (2017) Towards a secure service provisioning framework in a smart city environment. Future Generation Computer Systems 77: 112-135.

King, T. M., et al. (2019) AI for Testing Today and Tomorrow: Industry Perspectives. 2019 IEEE International Conference On Artificial Intelligence Testing (AITest).

Knapp, E. (2015) Cyber security in process plants: Recognizing risks, addressing current threats: As attacks on industrial control systems (ICSs) become more frequent and sophisticated, defensive strategies must evolve to keep up. Fortunately, the tools are getting better. Control Engineering 62(7): P6-P6.

Knieper, C. und C. Pahl-Wostl (2016) A comparative analysis of water governance, water management, and environmental performance in river basins. Water Resources Management 30(7): 2161-2177.

Koo, D., et al. (2015) Towards sustainable water supply: schematic development of big data collection using internet of things (IoT). Procedia Engineering 118: 489-497.

Koparan, C., et al. (2018) In Situ Water Quality Measurements Using an Unmanned Aerial Vehicle (UAV) System. Water 10(3): 264.

Kulkarni, S. A., et al. (2020) Intelligent Water Level Monitoring System Using IoT. 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC).

Kumar, N., et al. (2016) Ethical aspects and future of artificial intelligence. 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), IEEE.

Kumar, P., et al. (2021) An overview of monitoring methods for assessing the performance of nature-based solutions against natural hazards. Earth-Science Reviews 217: 103603.

KWB (2022) "SEMAplus: Altersvorsorge für Abwasserkanäle." Abgerufen von https://www.kompetenz-wasser.de/de/forschung/dienstleistungen/semaplus (01.06.2022).

L

L'Huillier, G., et al. (2010) Latent semantic analysis and keyword extraction for phishing classification. 2010 IEEE International Conference on Intelligence and Security Informatics.

Langeveld, J. G., et al. (2022) Urban drainage asset management – also for blue-green infrastructures!

Larsen, T. A., et al. (2021) The potential contribution of urine source separation to the SDG agenda–a review of the progress so far and future development options. Environmental Science: Water Research & Technology 7(7): 1161-1176.

Larsen, T. A., et al. (2016) Emerging solutions to the water challenges of an urbanizing world. Science 352(6288): 928-933.

Lasi, H., et al. (2014) Industry 4.0. Business & Information Systems Engineering 6(4): 239-242.

LAWA, et al. (2021) Fachkräftesicherung und -qualifizierung für die Wasserwirtschaft.

Lee, I. (2020) Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet 12(9): 157.

Lee, J., et al. (2020) Water-related disasters and their health impacts: A global review. Progress in Disaster Science 8: 100123.

Leps, O. (2018) Hybride Testumgebungen Für Kritische Infrastrukturen, Springer.

Leyden, J. (2016) "Water treatment plant hacked, chemical mix changed for tap supplies." Abgerufen von https://www.theregister.com/2016/03/24/water_utility_hacked/ (01.06.2022).

LIMES Security (2021) "AWT.103 Zero Downtime: Blackout Edition." Abgerufen von https://limessecurity.com/de/academy/awt-103/ (01.06.2022).

Lin, W.-C., et al. (2015) CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-Based Systems 78: 13-21.

Lu, Y. (2017) Industry 4.0: A survey on technologies, applications and open research issues. Journal of industrial information integration 6: 1-10.

Lu, Y. und L. D. Xu (2019) Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. IEEE Internet of Things Journal 6(2): 2103-2115.

Luque-Ayala, A. und S. Marvin (2016) The maintenance of urban circulation: An operational logic of infrastructural control. Environment and Planning D: Society and Space 34(2): 191-208.

Lv, Z. und S. Xie (2021) Artificial intelligence in the digital twins: State of the art, challenges, and future research topics. Digital Twin 1(12): 12.

M

Ma, W., et al. (2021) Applicability of a nationwide flood forecasting system for Typhoon Hagibis 2019. Scientific reports 11(1): 1-12.

Magloff, L. (2022) "VR used to create digital twin of German city."

Mahmoud, H. H. M., et al. (2019) Secure data aggregation mechanism for water distribution system using blockchain. 25th International Conference on Automation and Computing (ICAC), IEEE.

Makropoulos, C. und D. A. Savić (2019) Urban Hydroinformatics: Past, Present and Future. Water 11(10): 1959.

Mansfield-Devine, S. (2019) The state of operational technology security. Network security 2019(10): 9-13.

Marinelli, E., et al. (2021) Validation of an evidence-based methodology to support regional carbon footprint assessment and decarbonisation of wastewater treatment service in Italy. Water research 207: 117831.

Marquardt, U., et al. (2021) Teil 1: Was sich geändert hat. Der Branchenspezifische Sicherheitsstandard. Wasser/ Abwasser (Version 2021).

Martinez-Piazuelo, J., et al. (2020) A multi-critic reinforcement learning method: An application to multi-tank water systems. Ieee Access 8: 173227-173238.

Mathur, A. P. und N. O. Tippenhauer (2016) SWaT: A water treatment testbed for research and training on ICS security. 2016 international workshop on cyber-physical systems for smart water networks (CySWater), IEEE.

Maurer, M. und C. Ebi (o. J.) "Smart Water Pipes." Abgerufen von https://www.eawag.ch/de/abteilung/sww/projekte/smart-water-pipes/ (01.06.2022).

Mazzei, P. (2019) Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000. New York Times.

McDonald, W. (2019) Drones in urban stormwater management: a review and future perspectives. Urban Water Journal 16(7): 505-518.

Mehmood, H., et al. (2020) Strategic Foresight to Applications of Artificial Intelligence to Achieve Water-related Sustainable Development Goals.

Mendix (2019) "SUEZ launches the UK's first Self-Service Waste Management Customer Pricing Tool with Mendix." Abgerufen von https://www.mendix.com/press/suez-launches-the-uks-first-self-service-waste-management-customer-pricing-tool-with-mendix/ (01.06.2022).

Meney, K. A. und L. Pantelic (2022) Decentralized Water and Wastewater Systems for Resilient Societies: A Shift Towards a Green Infrastructure-Based Alternate Economy. The Palgrave Handbook of Climate Resilient Societies, Springer: 157-184.

Mercer, K. (2016) State of the Water Industry. AWWA 108: 63-73.

Microsoft (2016) Water Industry - Benefits of moving to Cloud technology.

Mishra, P., et al. (2020) Software defined internet of things security: properties, state of the

art, and future research. IEEE Wireless Communications 27(3): 10-16.

Mitchell, R. und I.-R. Chen (2014) A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv. 46(4): Article 55.

Montgomery, M. und T. Logan (2021) Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure, Foundation for Defense of Democracies Center on Cyber and Technology Innovation.

Motlagh, N. H., et al. (2020) Internet of Things (IoT) and the Energy Sector. Energies 13(2): 494.

Moy de Vitry, M., et al. (2018) Sewer Inlet Localization in UAV Image Clouds: Improving Performance with Multiview Detection. Remote Sensing 10(5): 706.

Mülbaier, M. (2021) Gute Perspektiven für Emscher und Lippe. gwf Wasser | Abwasser.

Müller, K. J. (2011) Sicherheit im Smart Grid. Karlsruhe: Secorvo Security Consulting GmbH.

Murillo, A., et al. (2020) Co-Simulating Physical Processes and Network Data for High-Fidelity Cyber-Security Experiments. Sixth Annual Industrial Control System Security (ICSS) Workshop. Austin, TX, USA, Association for Computing Machinery: 13–20.

N

Nazir, S., et al. (2015) Autonomous monitoring of critical infrastructures. 2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE).

NetApp (2018) Private Cloud Computing für die Wasserwirtschaft an Emscher und Lippe mit FlexPod Datacenter, NetApp.

Neumann, J., et al. (2021) Using observation and measured data to validate coupled 1D/2D flood models-first experiences from the project SENSARE. 15th International Conference on Urban Drainage. Melbourne.

Nikolopoulos, D., et al. (2020) Cyber-physical stress-testing platform for water distribution networks. Journal of Environmental Engineering 146(7): 04020061.

Nobles, C. (2018) Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration 9(3): 71-88.

O

Oracle Utilities (2019) The Acceleration of Cloud Computing for Utilities, Oracle Utilities.

Oral, H. V., et al. (2020) A review of nature-based solutions for urban water management in European circular cities: A critical assessment based on case studies and literature. Blue-Green Systems 2(1): 112-136.

Ornes, S. (2013) "The data flood." Abgerufen von https://www.sciencenewsforstudents.org/article/data-flood (01.06.2022).

OSIsoft (2017) Smart Water: Saving Millions and Cutting Energy By Combining IT and OT with the PI System.

Oyewumi, I. A., et al. (2019) Isaac: The idaho cps smart grid cybersecurity testbed. 2019 IEEE Texas Power and Energy Conference (TPEC), IEEE.

P

Pacchin, E., et al. (2019) A Comparison of Short-Term Water Demand Forecasting Models. Water Resources Management 33(4): 1481-1497.

Palleti, V. R., et al. (2021) Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecurity 4(1): 1-19.

Parsons, K., et al. (2014) Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security 42: 165-176.

Paudel, S., et al. (2013) Security standards taxonomy for Cloud applications in Critical Infrastructure IT. 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013).

Paul, J. D. und W. Buytaert (2018) Chapter One - Citizen Science and Low-Cost Sensors for Integrated Water Resources Management. Advances in Chemical Pollution, Environmental Management and Protection. J. Friesen und L. Rodríguez-Sinobas, Elsevier. 3: 1-33.

Pesantez, J. E., et al. (2022) Using a digital twin to explore water infrastructure impacts during the COVID-19 pandemic. Sustainable Cities and Society 77: 103520.

Pipebots (2021) "About." Abgerufen von http://pipebots.ac.uk/about/ (01.06.2022).

Poberezhna, A. (2018) Chapter 14 - Addressing Water Sustainability With Blockchain Technology and Green Finance. Transforming Climate Finance and Green Investment with Blockchains. A. Marke, Academic Press: 189-196.

Potsdam (o. J.) "Potsdam wird Smart City Modellkommune." Abgerufen von https://www.potsdam.de/potsdam-wird-smart-city-modellkommune#:~:text=Gr %C3 %BCn., %C3 %BCber %20die %20Bewilligung %20ihres %20F %C3 %B6rderantrags (01.06.2022).

PwC (2019) How AI can enable a Sustainable Future, Microsoft und PriceWaterhouseCoopers.

Q

Qi, Y., et al. (2020) Addressing Challenges of Urban Water Management in Chinese Sponge Cities via Nature-Based Solutions. Water 12(10): 2788.

R

Rabaey, K., et al. (2020) The third route: Using extreme decentralization to create resilient urban water systems. Water research 185: 116276.

Rajarajan, S. R. (2021) Risk assessment dashboard to visualize the cascading effects of critical infrastructure service failure due to natural hazards, University of Twente.

Ramani, S. K. und S. Iyengar (2017) Evolution of sensors leading to smart objects and security issues in iot. International Symposium on Sensor Networks, Systems and Security, Springer.

Rao, K. R., et al. (2018) IOT based water level and quality monitoring system in overhead tanks. International Journal of Engineering & Technology 7: 379.

Rasekh, A., et al. (2016) Smart water networks and cyber security, American Society of Civil Engineers. 142: 01816004.

Reed, J. (2021) "Can a small or medium size business be an "intelligent enterprise," or is it out of reach? SAP's Business ByDesign team makes its case."

Reeves, K. und C. Maple (2018) IoT interoperability: Security considerations and challenges in implementation. Living in the Internet of Things: Cybersecurity of the IoT - 2018.

Robles, T., et al. (2015) An IoT based reference architecture for smart water management processes. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 6(1): 4-23.

Rodriguez-Diaz, E., et al. (2015) Advanced smart metering infrastructure for future smart homes. 2015 IEEE 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), IEEE.

S

Sacyr (2022) "DIGITAL TWINS, THE VIRTUAL WATER REVOLUTION." Abgerufen von https://www.sacyr.com/en/-/gemelos-digitales-la-revolucion-virtual-del-agua (01.06.2022).

Saini, H. und A. Saini (2014) Security mechanisms at different levels in cloud infrastructure. International Journal of Computer Applications 108(2).

Sanchis, R., et al. (2020) Low-Code as Enabler of Digital Transformation in Manufacturing Industry. Applied Sciences 10(1): 12.

Sarabi, S. E., et al. (2019) Key Enablers of and Barriers to the Uptake and Implementation of Nature-Based Solutions in Urban Settings: A Review. Resources 8(3): 121.

Sarker, I. H., et al. (2021) AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science 2(3): 173.

Sarni, W., et al. (2018) Harnessing the fourth industrial revolution for water, World Economic Forum.

Sarni, W., et al. (2019) Digital water: Industry leaders chart the transformation journey. International Water Association and Xylem Inc.

Savić, D. (2021) Digital water developments and lessons learned from automation in the car and aircraft industries. Engineering.

Schieferdecker, I., et al. (2016) Urban data platforms: An overview. Proceedings of the 12th International Symposium on Open Collaboration Companion.

Schlaman, J. und F. Smal (2018) Smart Water Solutions - MANAGEMENT TREND: COMPREHENSIVE PLANNING & OPERATIONAL INTELLIGENCE SOLUTIONS DRIVE WATER SERVICE EFFICIENCY. Black & Veatch Strategic Directions. B. Veatch, Black & Veatch. WATER REPORT.

Schöller, M., et al. (2013) An Architectural Model for Deploying Critical Infrastructure Services in the Cloud. 2013 IEEE 5th International Conference on Cloud Computing Technology and Science.

Senatsverwaltung für Inneres, D. u. S. (2021) "Plan #B." Abgerufen von https://www.berlin.de/sen/inneres/sicherheit/innovation-wissenschaftsvernetzung-und-forschung/plan-b/plan-b-1129745.php (01.06.2022).

Services, T.-T. C. (2016) Cloud Adoption and UK Utilities, Tata consultancy services.

Shahzad, A., et al. (2014) Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption. Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication.

Shamsoshoara, A., et al. (2020) A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. Computer Networks 183: 107593.

Sharif, M., et al. (2016) Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. Proceedings of the 2016 acm sigsac conference on computer and communications security.

Shen, J., et al. (2017) A secure cloud-assisted urban data sharing framework for ubiquitous-cities. Pervasive and mobile Computing 41: 219-230.

Shin, S. W., et al. (2013) Fresco: Modular composable security services for software-defined networks. 20th annual network & distributed system security symposium, Ndss.

Shin, Y.-H., et al. (2021) Review—Recent Progress in Portable Fluorescence Sensors. Journal of The Electrochemical Society 168(1): 017502.

Singh, M. und S. Ahmed (2021) IoT based smart water management systems: A systematic review. Materials Today: Proceedings 46: 5211-5218.

Skybox Security (2021) Operational technology - cybersecurity risk significantly underestimated.

Slaughter, A. und P. Zonneveld (2017) An integrated approach to combat cyber risk - Securing industrial operations in oil and gas. D. C. f. E. Solutions, Deloitte Touche Tohmatsu Limited.

Slay, J. und M. Miller (2007) Lessons learned from the maroochy water breach. International conference on critical infrastructure protection, Springer.

Smart Energy International (2020) "Cloudy skies ahead for utilities." Abgerufen von https://www.smart-energy.com/industry-sectors/data_analytics/cloudy-skies-ahead-for-utilities-cloud-technologies/ (01.06.2022).

SmartCitiesWorld (2021) "Seoul uses AI to detect faults in city's sewer pipes." Abgerufen von https://www.smartcitiesworld.net/news/news/seoul-uses-ai-to-detect-faults-in-citys-sewer-pipes-6558 (01.06.2022).

Statista (2022) Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2022

Stevens, T. (2020) Knowledge in the grey zone: AI and cybersecurity. Digital War 1(1): 164-170.

Stewart, R. A., et al. (2018) Integrated intelligent water-energy metering systems and informatics: Visioning a digital multi-utility service provider. Environmental modelling & software 105: 94-117.

STOP-IT (2021) Empowering EU ISACs Project, ENISA and the JRCERNCIP Water group. WaterISAC knowledge sharing meeting & STOP-IT final event.

Strauss, M. und B. Wadzuk (2022) Predictive Maintenance of Stormwater Infrastructure Using Internet-of-Things Technology. Journal of Environmental Engineering 148(2): 04021084.

Sun, C. C., et al. (2021) Intrusion Detection for Cybersecurity of Smart Meters. IEEE Transactions on Smart Grid 12(1): 612-622.

T

Taddeo, M., et al. (2019) Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence 1(12): 557-560.

Tagabe, P. M. (2021) "Sydney Water's digital pillars to staying cyber safe." Abgerufen von https://utilitymagazine.com.au/sydney-waters-digital-pillars-to-staying-cyber-safe/ (01.06.2022).

Tank, D., et al. (2019) Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison. International Journal of Information Technology.

Taormina, R., et al. (2017) Characterizing cyber-physical attacks on water distribution systems. Journal of Water Resources Planning and Management 143(5): 04017009.

Taormina, R., et al. (2018) Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks. Journal of Water Resources Planning and Management 144(8): 04018048.

tendersUK (2021) "22/07/2021 Huntingdon: Cloud Hosting Services Framework. Anglian Water. 31000 000 GBP." Abgerufen von https://www.tenders-uk.com/22-07-2021-huntingdon-cloud-hosting-services-framework-anglian-water-31-000-000-gbp/ (01.06.2022).

Thio, S. K., et al. (2022) Lab on a smartphone (LOS): A smartphone-integrated, plasmonic-enhanced optoelectrowetting (OEW) platform for on-chip water quality monitoring through LAMP assays. Sensors and Actuators B: Chemical 358: 131543.

Thomas, J. (2020) "Why Utilities Industry Is Moving To Cloud Computing." Abgerufen von https://medium.com/@mikethomsan/utilities-industry-moving-to-cloud-computing-4caa5afee868#:~:text=With %20cloud %20technology %2C %20utilities %20can,joint %20enterprise %2C %20and %20partnership %20arrangements (01.06.2022).

Trend Micro (2015) Report on Cybersecurity and Critical Infrastructure in the Americas, Organization for American States.

Tu, H., et al. (2020) Cascading Failures of Power System with the Consideration of Cyber Attacks. 2020 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE.

Tufan, E., et al. (2021) Anomaly-Based Intrusion Detection by Machine Learning: A Case Study on Probing Attacks to an Institutional Network. Ieee Access 9: 50078-50092.

Tunc, C., et al. (2015) Teaching and training cybersecurity as a cloud service. 2015 International Conference on Cloud and Autonomic Computing, IEEE.

Tuptuk, N., et al. (2021) A systematic review of the state of cyber-security in water systems. Water 13(1): 81.

U

Umweltbundesamt, U. (2021) Direkte und indirekte Umwelteffekte von intelligenten, vernetzten urbanen Infrastrukturen, Umweltbundesamt.

UNESCO (2021) "International Initiative on Water Quality (IIWQ)." Abgerufen von https://en.unesco.org/waterquality-iiwq/wq-challenge (01.06.2022).

UP KRITIS (2014) UP KRITIS - Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen. B. f. S. i. d. Informationstechnik. Bonn, Geschäftsstelle des UP KRITIS.

UP KRITIS (2020) Empfehlungen zur Nutzung von Cloud-Dienstleistungen in Kritischen Infrastrukturen. Themenarbeitskreis "Nutzung cloudbasierter Dienste" des UP KRITIS.

V

Vellaithurai, C., et al. (2013) SECPSIM: A Training Simulator for cyber-power infrastructure security. 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm).

Vikesland, P. J. (2018) Nanosensors for water quality monitoring. Nature Nanotechnology 13(8): 651-660.

Vincent, J. (2020) "Google's AI flood warnings now cover all of India and have expanded to Bangladesh." Abgerufen von https://www.theverge.com/2020/9/1/21410252/google-ai-flood-warnings-india-bangladesh-coverage-prediction (01.06.2022).

Visio.ai (o. J.) Abgerufen von https://viso.ai/computer-vision/low-code-ai-for-computer-vision/#:~:text=Low %2Dcode %2Fno %2Dcode %20machine %20learning %20platforms %20allow %20non,to %20hard %2Dcoded %20programming %20techniques (01.06.2022).

W

Wang, S. P., et al. (2017) Security by Design: Defense-in-Depth IoT Architecture. Journal of The Colloquium for Information Systems Security Education 4.

Wang, Y.-C., et al. (2020) Pore-Confined Silver Nanoparticles in a Porphyrinic Metal–Organic Framework for Electrochemical Nitrite Detection. ACS Applied Nano Materials 3(9): 9440-9448.

Water Intelligence (o. J.) "Solutions." Abgerufen von https://waterintelligence.co.uk/solutions/ (01.06.2022).

X

Xiaocong, M., et al. (2015) An IoT-based system for water resources monitoring and management. 2015 7th International Conference on Intelligent Human-Machine Systems and Cybernetics, IEEE.

Xu, T., et al. (2014) Security of IoT systems: Design challenges and opportunities. 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), IEEE.

Y

Young, R. (2013) Saving Water and Energy Together: Helping Utilities Build Better Programs, American Council for an Energy-Efficient Economy.

Younis, Y. A. und K. Kifayat (2013) Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep: 28.

Z

Zaalouk, A., et al. (2014) OrchSec: An orchestrator-based architecture for enhancing network-security using network monitoring and SDN control functions. 2014 IEEE Network Operations and Management Symposium (NOMS), IEEE.

Zhang, K., et al. (2017) Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine 55(1): 122-129.

Zhang, S., et al. (2022) Practical Adoption of Cloud Computing in Power Systems -Drivers, Challenges, Guidance, and Real-world Use Cases. IEEE Transactions on Smart Grid: 1-1.

Zimmermann, M., et al. (2020) Siedlungswasserwirtschaft im Zeitalter der Digitalisierung: Cybersicherheit als Achillesferse. TATuP-Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis/Journal for Technology Assessment in Theory and Practice 29(1): 37-43.

Zou, X.-Y., et al. (2019) A novel event detection model for water distribution systems based on data-driven estimation and support vector machine classification. Water Resources Management 33(13): 4569-4581.

Impressum

Herausgeber
Kompetenzzentrum Wasser
Berlin gGmbH
Cicerostrasse 24
10709 Berlin
www.kompetenz-wasser.de

Geschäftsführer
Jochen Rabe

Verfasser:innen
Dr. Nicolas Caradot
Gruppenleitung
Nicolas.Caradot@kompetenz-wasser.de
+ 49 (0)151 1657 6048

Nikolaus de Macedo Schäfer
Wissenschaftlicher Mitarbeitender
Nikolaus.Schaefer@kompetenz-wasser.de
+49 (0)177 4410526

Elina Henning
Praktikantin

Prüfer:innen
Jean Kolarow
Pascale Rouault

Redaktion
Franziska Sahr

Grafische Umsetzung
Bianca Cramer
Nikolaus de Macedo Schäfer

Bildnachweis:
Cover: Michael Matton via Unsplash
S. 5: Tony Wan via Unsplash
S. 6: Midhun Harikumar via Unsplash
S. 10: Hanbyul Jeong via Unsplash
S. 19: Luis Vidal via Unsplash
S. 20: Jorge Ramirez & Claire Fischer via Unsplash
S: 26: Bret Kavanaugh via Unsplash
S. 32: Yosh Ginsu & Markus Spiske via Unsplash
S. 39: Iryna Dazhura
S. 40: Ivan Bandura via Unsplash
S. 46: Clark Hua via Unsplash
S. 53: Marlo Wock via Unsplash
S. 54: Mitya Ivanov via Unsplash
S. 60: Marissa Rodriguez via Unsplash
S. 65: Adi Goldstein via Unsplash
S. 66: Kerem Karaarslan via Unsplash

Haftungsausschluss
Die in dieser Publikation bereitgestellte Information wurde zum Zeitpunkt der Erstellung im Konsens mit den bei Entwicklung und Anfertigung des Dokumentes beteiligten Personen als technisch einwandfrei befunden. KWB schließt vollumfänglich die Haftung für jegliche Personen-, Sach- oder sonstige Schäden aus, ungeachtet ob diese speziell, indirekt, nachfolgend oder kompensatorisch, mittelbar oder unmittelbar sind oder direkt oder indirekt von dieser Publikation, einer Anwendung oder dem Vertrauen in dieses Dokument herrühren. KWB übernimmt keine Garantie und macht keine Zusicherungen ausdrücklicher oder stillschweigender Art bezüglich der Richtigkeit oder Vollständigkeit jeglicher Information hierin. Es wird ausdrücklich darauf hingewiesen, dass die in der Publikation gegebenen Informationen und Ergebnisse aufgrund nachfolgender Änderungen nicht mehr aktuell sein können. Weiterhin lehnt KWB die Haftung ab und übernimmt keine Garantie, dass die in diesem Dokument enthaltenen Informationen der Erfüllung Ihrer besonderen Zwecke oder Ansprüche dienlich sind. Mit der vorliegenden Haftungsausschlussklausel wird weder bezweckt, die Haftung der KWB entgegen den einschlägigen nationalen Rechtsvorschriften einzuschränken noch sie in Fällen auszuschließen, in denen ein Ausschluss nach diesen Rechtsvorschriften nicht möglich ist.

© Copyright 2022 by the
Kompetenzzentrum Wasser Berlin gGmbH
All rights including translation into other languages, reserved under the Universal Copyright Convention, the Berne Convention or the Protection of Literacy and Artistic Works, and the International and Pan American Copyright Conventions.

Present report was developed in compliance with the requirements of the quality management system DIN EN ISO 9001:2015

KWB

Kompetenzzentrum *W*asser Berlin
gemeinnützige GmbH