TNO innovation for life

Een verkenning voor de Nederlandse watersector

Cyber Ranges en Digital Twins

TNO Publiek ⟩ TNO 2023 R11186
augustus 2023

Defence, Safety & Security
www.tno.nl
+31 88 866 10 00
info@tno.nl

TNO 2023 R11186 – augustus 2023

Cyber Ranges en Digital Twins

Een verkenning voor de Nederlandse watersector

Auteurs	M.P. de Bakker, M.H.A. Klaver, J.P. Konijn, E.A.F. Langius, E. Lazovik, H.B. Meeuwissen, S. Mergler, T. van Schie
Rubricering rapport	TNO Publiek
Bijlagen	TNO Publiek
Aantal pagina's	67 (excl. voor- en achterblad)
Aantal bijlagen	2
Projectnaam	Verkenningsstudie Cyber Ranges en Digital Twins
Projectnummer	060.56475

Samenvatting

De Nederlandse watersector staat voor verscheidene cyberuitdagingen. Cybersecurity is een steeds belangrijker onderwerp voor de watersector geworden, omdat:

1. Digitale dreigingen toenemen. Dreigingen kunnen leiden tot verstoringen van de watervoorziening, schade aan kritieke infrastructuur en mogelijke inbreuken op de veiligheid van de bevolking.
2. In de watersector onder andere verouderde (OT-)systemen draaien. Deze kunnen kwetsbaar zijn voor cyberaanvallen.
3. De regulering op het gebied van cybersecurity voor organisaties in de vitale sector toeneemt (bijvoorbeeld NIS2[1], CSIR[2], CSA[3]).

Om deze cyberuitdagingen het hoofd te bieden is het essentieel dat de watersector blijft innoveren en investeren in sterke cybersecuritymaatregelen. Onder het programma 'Versterken van de cyberweerbaarheid in de watersector' van het Ministerie van Infrastructuur en Waterstaat (I&W) heeft TNO daarom in deze verkenningsstudie onderzocht hoe twee innovatieve technologieën, Cyber Ranges en Digital Twins, een bijdrage kunnen leveren in het verhogen van de cyberweerbaarheid van de Nederlandse watersector.

De studie omvat een algemene literatuurverkenning om de verschillende definities van Digital Twins en Cyber Ranges in kaart te brengen. Om een beeld te krijgen in hoeverre deze technologieën al in de watersector toegepast worden is een verdiepende literatuurverkenning uitgevoerd en zijn enkele experts binnen de watersector geïnterviewd (Het Waterschapshuis, Rijkswaterstaat, Vitens). Vervolgens is specifiek onderzoek gedaan naar de toepassing van Digital Twins en Cyber Ranges op het gebied van cybersecurity. Hiervoor zijn tevens voorbeelden uit sectoren buiten de watersector bekeken.
In brainstorming-sessies met TNO experts vanuit verschillende onderzoeksgroepen is gezamenlijk verkend welke kansen, dan wel denkrichtingen, Digital Twin en Cyber Range toepassingen in de Nederlandse watersector kunnen hebben.

De resultaten van deze verkenningsstudie laten zich als volgt samenvatten:

1. Hoewel er verschillende definities van Cyber Ranges en Digital Twins bestaan en de afbakening tussen de twee technologieën niet altijd even duidelijk is, hebben wij kunnen aantonen dat het belangrijkste verschil tussen de twee technologieën in het gebruik ligt: Een Cyber Range is hoofdzakelijk ontworpen voor cybersecurity-training en -simulatie. Het biedt een gecontroleerde omgeving om cyberaanvallen te simuleren, verdedigingsmechanismen te testen en professionals op te leiden in het reageren op en beperken van beveiligingsbedreigingen. Daarnaast wordt een Cyber Range ingezet bij het testen van (nieuwe) netwerkapparatuur en (nieuwe) processen.

[1] RICHTLIJN (EU) 2022/2555 VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn)
[2] CyberSecurity ImplementatieRichtlijn
[3] VERORDENING (EU) 2019/881 VAN HET EUROPEES PARLEMENT EN DE RAAD van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening)

Digital Twins daarentegen richten zich niet specifiek op het cybersecurity-domein. Een Digital Twin wordt gebruikt voor de optimalisatie van primaire operationele bedrijfsprocessen door een virtuele representatie te maken van een fysiek object, proces of systeem om de prestaties van de echte entiteit die het vertegenwoordigt te monitoren, analyseren en optimaliseren.

2. In de watersector zijn wereldwijd tot nu toe alleen enkele voorbeelden van Cyber Ranges bekend. De Nederlandse watersector maakt momenteel nog geen gebruik van een Cyber Range die specifiek ontworpen is voor de watersector.

3. Digital Twins worden zowel in het binnen- als buitenland in de watersector toegepast voor de optimalisatie van primaire bedrijfsprocessen. In de academische wereld is één voorbeeld gevonden waarin een open-source Digital Twin van een drinkwater distributie system gebruikt kan worden voor cybersecurity-doeleinden. Er zijn wereldwijd echter geen Digital Twins bekend die voor cybersecurity-doeleinden in de watersector ingezet worden.

4. Beide technologieën bieden een aantal kansen, dan wel denkrichtingen, om de Nederlandse watersector meer cyberweerbaar te maken:
   - Kans 1. Een watersector-specifieke Cyber Range voor training van personeel.
   - Kans 2. Een Cyber Range voor het oefenen en verbeteren van incident-response procedures.
   - Kans 3. Een Cyber Range in een OTAP-omgeving[4] om cyberrobuustheid en -gedrag van nieuwe componenten te testen.
   - Kans 4. Een Cyber Range voor het experimenteren met gepubliceerde kwetsbaarheden.
   - Kans 5. Een Cyber Range met een geïntegreerde Digital Twin om effecten van cyberaanvallen op primaire bedrijfsprocessen te simuleren.
   - Kans 6. Een Digital Twin voor het detecteren van anomalieën en cyberaanvallen in real-time.

Kans 5 is als meest waardevol beoordeeld tijdens de presentatie van de bevindingen. Bij de presentatie waren experts van het Ministerie I&W en vertegenwoordigers uit de watersector aanwezig. Kans 3 (dicht gevolgd van kans 2 en 5) werd gezien als kans die het beste kan ondersteunen om aan wetgeving en richtlijnen in de watersector te voldoen.

[4] OTAP: Ontwikkel-, Test-, Acceptatie-, Productieomgeving.

Inhoudsopgave

1 Inleiding

De digitalisering in vitale processen neemt een grote vlucht. Fabrikanten en ontwikkelaars leveren componenten, software en diensten die eigenaren van vitale processen gebruiken om de kansen digitalisering biedt te benutten. Beheerders van vitale processen hebben baat bij deze digitalisering. Bijvoorbeeld omdat het ze in staat stelt om op afstand temperatuursensoren te laten uitlezen en deze data te gebruiken om automatisch handelingen uit te laten voeren op een andere plek in het proces. Rijkswaterstaat, waterschappen en drinkwaterbedrijven maken allemaal gebruik van kantoorautomatisering en machines die aangestuurd worden door ICS (Industrial Control Systems) of OT, de zogenaamde Operationele Techniek (OT).[5] Voor Nederland is de watersector van groot belang en actoren in de sector zijn grotendeels aangemerkt als een vitaal proces. Hierbij wordt de volgende onderverdeling aangehouden:

- Drinkwatervoorziening, gericht op de continue levering van goed drinkwater. Hiervoor zijn de 10 drinkwaterbedrijven verantwoordelijk;
- Keren en beheren waterkwantiteit: het beschermen van Nederland tegen hoog water. Hiervoor zijn Rijkswaterstaat (RWS) en de waterschappen verantwoordelijk.

Voor deze vitale processen is de cyberweerbaarheid van groot belang. Het programma ‘Cyberweerbaarheid in de Watersector’ richt zich op het identificeren van mogelijkheden om de cyberweerbaarheid van de watersector te versterken. ICT-systemen in de watersector raken gaandeweg meer verweven met ICS. Installaties raken daardoor afhankelijker van digitale processen en deze trend zal zich voortzetten.

Het Ministerie van Infrastructuur en Waterstaat (I&W) heeft als doelstelling dat het “streeft naar het op orde houden van een duurzaam watersysteem tegen maatschappelijk aanvaardbare kosten. Dat houdt in dat Nederland daarmee droge voeten heeft, over voldoende zoetwater beschikt en schoon (drink)water heeft en kan blijven gebruiken.” Het in de gaten houden van trends en ontwikkelingen die bijdragen aan verbetering van de continuïteit (bijv. relevante hulpmiddelen en technologieën) is een van de manieren om deze doelstelling te behalen.

Cyber Ranges en Digital Twins zijn technologieën die in andere domeinen reeds toegepast worden. Cyber Ranges helpen organisaties zoals bijvoorbeeld defensie als trainingsfaciliteit om meer cyberweerbaar te worden. Digital Twins worden ingezet om bedrijfsprocessen te optimaliseren. Digital Twins hebben hun intocht al in de Nederlandse watersector gemaakt, al dan niet specifiek in de context van cybersecurity.[6] Zo maakt drinkwaterbedrijf Vitens bijvoorbeeld gebruik van een Digital Twin om de efficiëntie in de productie en distributie van drinkwater te verbeteren. Omdat in de watersector tot op heden nog geen gezamenlijk initiatief is genomen om de mogelijkheden van Digital Twins en Cyber Ranges op het gebied

[5] Naast deze twee termen wordt ook vaak de term SCADA-systemen (SCADA staat voor Supervisory Control and Data Acquisition) gebruikt. Zie toelichting van deze terminologie in hoofdstuk 3.4.

[6] Definitie cybersecurity van het Cybersecurity woordenboek: “Alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of herstellen als die toch is ontstaan. Voorbeelden van schade zijn dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen.”

van cybersecurity te onderzoeken, voert TNO een verkenningsstudie uit in opdracht van IenW naar deze twee technologieën en toepassingsmogelijkheden voor de Nederlandse watersector. Kunnen deze technologieën een bijdrage leveren aan het vergroten van de cyberweerbaarheid van de Nederlandse watersector? Zo ja, op welke manier(en)?

Het onderzoeksrapport behandelt daarvoor de volgende vier onderzoeksvragen:
1. Wat zijn Cyber Ranges en Digital Twins en wat is het probleem dat met Digital Twins en Cyber Ranges opgelost kan worden (toepassingsmogelijkheden)?
2. Wordt er zowel in theorie als praktijk onderscheid gemaakt tussen de technologische vereisten van Digital Twin en Cyber Range technologieën afhankelijk van de gekozen toepassing?
3. Zijn er wereldwijd best practices of voorbeelden van onderzoeks- en of innovatieprojecten op het gebied van Cyber Ranges en Digital Twins in de watersector en andere sectoren, en wat kan de Nederlandse watersector hiervan leren?
4. Wat zijn de randvoorwaarden om Cyber Ranges of Digital Twins in de praktijk toe te kunnen passen?

Succesvolle cyberaanvallen op digitale systemen in de watersector kunnen leiden tot grote economische en maatschappelijke impact. In wetenschappelijke tijdschriften en (online) media is een aantal internationale cybersecurity-incidenten in de watersector beschreven. In bijlage A zijn deze kort samengevat. Voor zover publiek bekend heeft de Nederlandse watersector tot nu toe geen last gehad van grote cyberincidenten die invloed hebben gehad op primaire (bedrijfs)processen. De sector probeert echter wel, net zoals vele andere sectoren, haar primaire (bedrijfs)processen zo goed mogelijk te beschermen. “Bij het keren en beheren van water staat de fysieke veiligheid van Nederland op het spel: in de strijd met het water kan het gaan om leven of dood. [1]”. Het cyberweerbaar maken van die processen is dan ook van belang en daarvoor wordt gekeken naar nieuwe technologieën.

De resultaten van dit onderzoek naar Cyber Ranges en Digital Twins kunnen worden gebruikt om te bepalen of deze twee technologieën in Nederland een bijdrage kunnen leveren aan het behouden van droge voeten, voldoende zoet water en schoon (drink)water.

1.1 Onderzoeksmethode

De resultaten van dit rapport zijn tot stand gekomen door toepassing van verschillende onderzoeksmethodes. In dit project is een algemene literatuurverkenning uitgevoerd om de verschillende definities van Digital Twins en Cyber Ranges in kaart te brengen. Om een beeld te krijgen in hoeverre Digital Twins en Cyber Ranges tegenwoordig al in de watersector toegepast worden is een verdiepende literatuurverkenning uitgevoerd en zijn enkele experts binnen de watersector geïnterviewd (Het Waterschapshuis, Rijkswaterstaat, Vitens). Vervolgens werd specifiek onderzoek gedaan naar de toepassing van Digital Twins en Cyber Ranges op het gebied van cybersecurity. Hiervoor zijn tevens voorbeelden uit sectoren buiten de watersector bekeken. In brainstorming-sessies met TNO experts vanuit verschillende afdelingen werd gezamenlijk verkend welke kansen, dan wel denkrichtingen, Digital Twin en Cyber Range toepassingen in de Nederlandse watersector kunnen hebben. De TNO-experts brachten hiervoor ideeën en ervaring in vanuit verschillende expertisegebieden: Digital Twin, Cyber Range, cybersecurity, en watersector.

De resultaten van dit onderzoek zijn op 19 juni 2023 gepresenteerd aan experts bij het Ministerie I&W en vertegenwoordigers uit de watersector. Tijdens de presentatie is het publiek op een interactieve manier via Menti-meter bevraagd naar hun bevindingen ten opzichte van de resultaten van dit onderzoek, in het bijzonder naar hun mening over de

kansen zoals beschreven in hoofdstuk 6. De verkregen informatie is toegevoegd aan bijlage B.

2 Definities

Voor zowel Cyber Range als ook Digital Twin zijn meerdere definities in omloop. Een aantal daarvan en hun kenmerken worden in de hoofdstukken 3 en 4 nader toegelicht. In dit TNO rapport hanteren wij de volgende definities:

- ***Cyber Range*** definitie volgens ECSO*:* "A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases [2]."

- ***Digital Twin*** definitie volgens WUR*:* "Een Digital Twin is de combinatie en interactie van een fysiek systeem (zoals een autofabriek) en een virtuele representatie van dit systeem, vaak een computermodel. De Digital Twin wordt gevoed met continue datastromen vanuit het fysieke systeem, zodat een accurate en actuele virtuele representatie van het systeem ontstaat. Deze digitale kopie kan op haar beurt weer communiceren met het fysieke systeem, om zo controle uit te oefenen en het systeem naar een gewenste toestand te sturen. Ook kan een Digital Twin virtueel verschillende scenario's analyseren, zodat men weet wat te doen indien deze scenario's optreden in het fysieke systeem [3]."

3 Begrippenkader Cyber Range

3.1 Definitie en toepassing

Binnen de literatuur bestaan er meerdere definities van het begrip “Cyber Range”. In deze paragraaf bespreken we drie verschillende definities.

Volgens het *National Institute of Standards and Technology (NIST)* worden Cyber Ranges gedefinieerd als: "Cyber Ranges are interactive, simulated representations of an organization’s local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing [4] [5]." Deze definitie geeft aan dat een Cyber Range een combinatie kan zijn van zowel hardware als software of een combinatie van beiden. Verder stelt NIST dat een Cyber Range kan bestaan uit zowel, originele (fysieke) hardware- en software componenten, als een hybride samenstellen van werkelijke en virtuele componenten.

Binnen deze context kan de gebruikersgroep zeer divers zijn, bestaande uit onder meer, studenten, professionals, docenten, en organisaties. Volgens NIST kunnen studenten, bijvoorbeeld gebruik maken van Cyber Ranges om hun kennis toe te passen in een gesimuleerde omgeving, of om gezamenlijk in teamverband cyberproblemen op te lossen en op die manier hun cyber-vaardigheden te ontwikkelen. Op vergelijkbare wijze kunnen organisaties Cyber Ranges toepassen om personeel op te leiden in nieuwe organisatorische en technische omgevingen, nieuwe procedures te testen zoals protocollen, of om cybercapaciteiten van personeel te toetsen.

Een andere veel gebruikte definitie binnen de literatuur is afkomstig van de *European Cyber Security Organisation (ECSO),* zoals al beschreven in het vorige hoofdstuk. De gebruikersgroep kan volgens deze definitie zeer divers zijn en bestaan uit: bedrijven, (strategische) beleidmakers, security professionals, defensie, militaire agentschappen, Security Operations Centra, studenten, onderzoekers, leerkrachten en opleiders [2].

Vergelijkbaar aan de voorgaande definitie is de begripsbepaling gegeven door KPN die gesteld is als volgt [6]: “Een Cyber Range is een gecontroleerde, interactieve technologische omgeving waar gebruikers kunnen leren en testen hoe ze cyberaanvallen kunnen detecteren en afzwakken met dezelfde apparatuur als die waarmee ze op het werk te maken krijgen. Cyber Ranges kunnen namelijk IT-systemen simuleren zonder bestaande netwerken te belasten. Op deze manier wordt de technische kennis rondom cyberresponse bij aanvallen vergroot.”

Er worden dus verschillende definities van een Cyber Range gehanteerd. Het ontbreken van een algemeen aanvaarde definitie heeft geleid tot uiteenlopende interpretaties en toepassingen van de term, ook in de gevonden literatuur. Dit blijkt ook uit de verslaglegging van CyberSec4Europe [7] en ESCO [2]. Zo wordt er gesteld dat Cyber Ranges niet gemakkelijk

met elkaar kunnen worden vergeleken wat betreft de kenmerken functionaliteiten, capaciteiten, diensten, en kenmerken, door het ontbreken van een wereldwijd overeengekomen alomvattende taxonomie van Cyber Ranges. Cyber Ranges, die pas enkele jaren bestaan kunnen voor reeks verschillende doeleinden worden toepast, en zijn dan ook in hoge mate configureerbaar en kunnen worden gebruikt in use-cases als [2]:

- Cybersecurity-testing;
- Cybersecurity-onderzoek;
- Cybersecurity-opleiding & training;
- Ontwikkeling en beoordeling van cyberweerbaarheid;
- Recruitment van (cyber)talent;
- Nationale en Internationale cybersecurity-competities.

Cyber Ranges kennen dus een breed scala aan toepassingen en use-cases en bieden meer dan louter een simulatieomgeving. Het definiëren van een Cyber Range als slechts een simulatieomgeving omvat niet de volledige complexiteit en unieke aspecten van een Cyber Range, aldus het rapport van ECSO. Het rapport illustreert dat er binnen de verschillende internationale definities van een Cyber Range over het algemeen twee benaderingen naar voren komen om een Cyber Range te definiëren.

De eerste benadering beschouwt een Cyber Range voornamelijk als een simulatieomgeving van een digitale infrastructuur die voornamelijk voor opleidings- en trainingsdoeleinden op het gebied van cybersecurity wordt ontwikkeld, en dus een statischere benadering is volgens ECSO.

De tweede benadering die in het rapport wordt geïntroduceerd, is een dynamische benadering van een Cyber Range, waarbij een Cyber Range wordt beschouwd als een platform van technologieën die voor een bredere scala van doeleinden gebruikt kan worden, zoals te zien is aan bovenstaande lijst met use-cases. Volgens de auteurs ligt de nadruk hier op het “gebruik”, en laat zich een simulatieomgeving pas door haar toepassing voor één van de use-cases als een Cyber Range definiëren. Zo is het van belang voor effectief gebruik van een Cyber Range voor verschillende doeleinden, dat een Cyber Range aanvullende capaciteiten biedt en functionaliteiten ter beschikking stelt aan de eindgebruiker om het creëren en het gebruik van verschillende simulatieomgevingen te vergemakkelijken. De mate van flexibiliteit bij het creëren van verschillende simulatieomgevingen en de omvang van de aangeboden functionaliteiten kunnen variëren tussen verschillende Cyber Ranges.

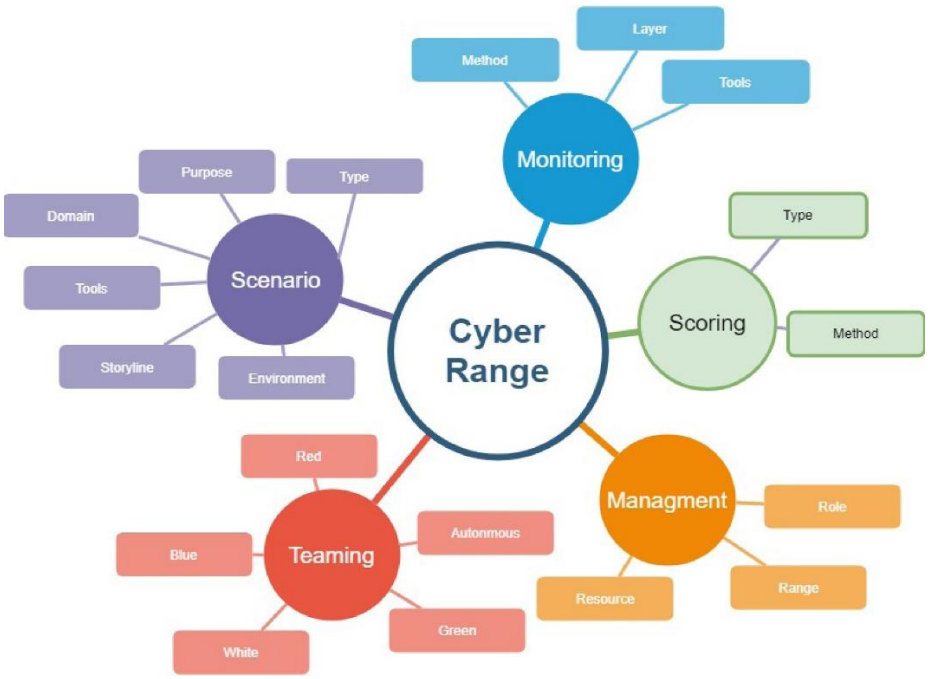
Dat er verschillende definities terugkomen observeren wij ook in de verschillende taxonomieën die worden opgesteld rondom Cyber Ranges [8] [9] in de literatuur. In het licht van de uiteenlopende definities van Cyber Ranges en ter bevordering van de duidelijkheid in dit rapport zullen voor het vervolg gebruik maken van de definitie van ECSO. Deze is voortgekomen uit een werkgroep van ECSO (WG5), met een brede groep van Europese partners (RTO’s, bedrijven) actief in het cybersecurity-domein. Het is dus een definitie die aansluiting vindt bij Europose bedrijven en instanties, die een bredere benadering van het begrip geeft dan andere definities.

3.2 Hoofdelementen van een Cyber Range

Yamin et al. [8] introduceren in hun paper *Cyber Ranges and security testbeds: Scenarios, functions, tools and architectures* een Cyber Range taxonomie op basis van een literatuur survey van 100 publicaties in de periode 2002 tot en met 2019 (zie figuur 3.1). De taxonomie beschrijft de volgende zes hoofdconcepten:

1. **Environment.** De omgeving die binnen een Cyber Range kan worden nagebootst. Zo kan de omgeving volgens de onderzoekers zowel hard- als software, gevirtualiseerde en gesimuleerde elementen bevatten. Zo stellen de onderzoekers dat hardware vaak toegepast wordt voor specifieke apparatuur, zoals Programmable Logic Controllers (PLCs) die veelal moeilijk te emuleren of te simuleren zijn.
2. **Scenario**. Het creëren, genereren, bewerken, inzetten en uitvoeren van cybersecurity-scenario's. In sommige Cyber Ranges bevatten specifieke componenten in hun architectuur voor de ontwikkeling van nieuwe scenario's.
3. **Monitoring**. Het loggen, monitoren, en verzamelen van informatie over de Cyber Range omgeving. Hierbij worden volgens de auteurs binnen de literatuur een breed scala van monitoring tooling gebruikt.
4. **Learning**. Hiermee kunnen de gebruikers van de Cyber Range leer- en tutorialmateriaal verkrijgen voor de belangrijkste reden: training. Deze Cyber Range capaciteit kan bestaan uit bijvoorbeeld instructie teksten, afbeelding of andere multimedia. Ook laten de auteurs zien dat sommige Cyber Ranges geïntroduceerd in de literatuur gebruik kunnen maken van scoremechanisme en andere hulpmiddelen om voortgang van de deelnemer of gebruikers bij te kunnen houden.
5. **Teaming** geeft de mogelijk voor gebruikers om deel te nemen in een teamverband. De auteurs [8] stellen dat teamverbanden in de verschillende constellaties deel kunnen nemen. Zo kan er in een blue en red team verband binnen een Cyber Range geacteerd worden. Bovendien, kan er ook een autonomous team zijn, waarbij, bepaalde activiteiten binnen de Cyber Range volledig geautomatiseerd zijn.
6. **Management** van een Cyber Range. Hier beschrijven de experts dat management veelomvattend kan zijn, maar voornamelijk betrekking heeft op de staat van de Cyber Range. Zo hebben sommige Cyber Ranges grafische interfaces om de Cyber Range in te stellen en te beheren. Maar kunnen er ook via deze interfaces nieuwe gebruikersrollen toegewezen worden, nieuwe apparaten toegevoegd worden, of application programming interface (API) toegang verleend worden.

Een Cyber Range hoeft niet in alle gevallen te voldoen aan de 6 hoofdcomponenten gepresenteerd in deze taxonomie. Zo zijn er voorbeelden genoemd in hoofdstukken 5.1 en 5.3 van dit rapport die geen learning, maar wel de andere concepten zoals monitoring, simulatie (environment), teaming, management, en ondersteuning voor scenario's bevat. Afhankelijk van het beoogde doel van de Cyber Range kunnen nog extra functionaliteiten wenselijk zijn. Hiervoor kan de integratie van systemen en toepassingen van derden met de Cyber Range nodig zijn.



Figuur 3.1: Cyber Range taxonomie. Uit [8].

Bovenstaand figuur illustreert in aanvulling op de hierboven beschreven taxonomie de verschillende technische componenten en functionaliteiten van een Cyber Range [2]. Het rapport van de ESCO geeft figuur 3.2 als voorbeeldarchitectuur en bevat verschillende technische componenten die een Cyber Range kan omvatten. Wij bespreken kort de meest belangrijke componenten van een Cyber Range [9, 2].

Orchestration: verantwoordelijk voor de automatische configuratie en het beheer van de onderliggende computersystemen. Zo wordt gesteld dat deze laag verantwoordelijk is voor automatiseringsworkflows, waarbij meerdere virtuele omgevingen gecreëerd, gemanaged en verwijderd kunnen worden. Daarnaast functioneert Orchestration als laag die automatisering tussen virtuele omgevingen mogelijk maakt, verschillende componenten van de Cyber Range automatiseert, bepaalde scenario's start, of interacties tussen de verschillende onderdelen mogelijk maakt, afhankelijk van de specifieke use-cases.

Internet Service Simulation: Gesimuleerde internetdiensten waar de Cyber Range zelf afhankelijk van is om een realistische omgeving te creëren. Bijvoorbeeld het simuleren van sociale mediaplatformen met als doel om het realisme van een specifieke use-case of scenario te vergroten.

Attack Simulation: De mogelijkheid om binnen de Cyber Range omgeving (cyber)aanvallen te simuleren.

User Activity Simulation: Het vermogen om het normale gedrag van goedaardige gebruikers te simuleren is naast het simuleren van de systemen en toepassingen van groot belang om zo een realistische omgeving te kunnen creëren. Voorbeelden van verschillende gebruikers-activiteiten kan zijn:

- Internetgedrag van gebruikers;
- Gebruikers die e-mails versturen.

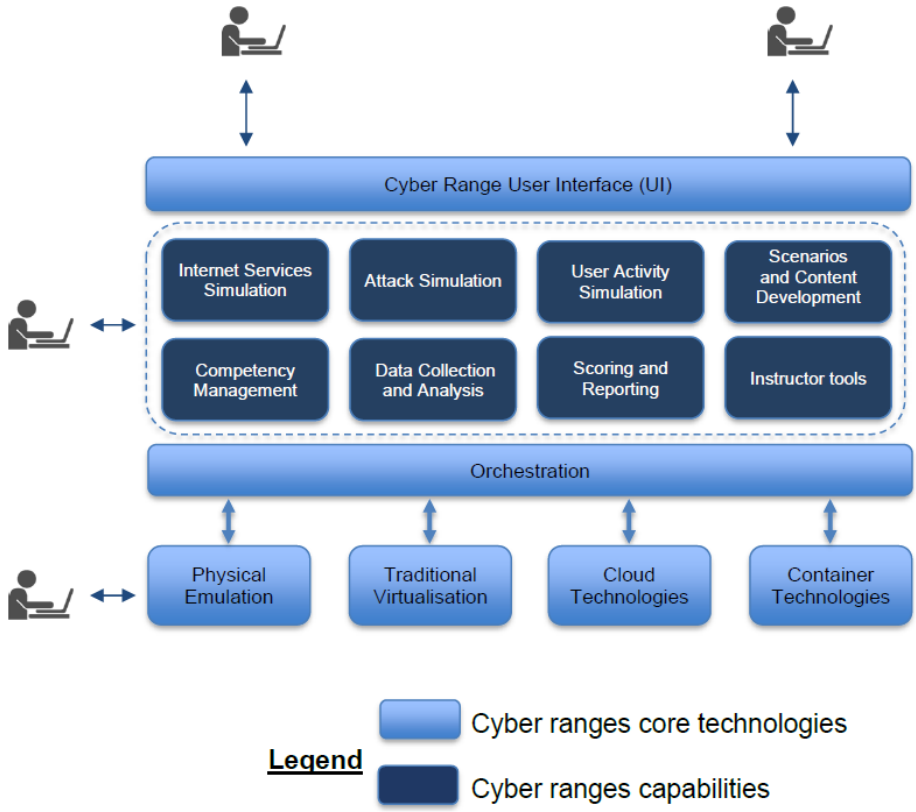
Scenario's and Content development: De mate waarin een Cyber Range toepasbaar of relevant is wordt aanzienlijk beïnvloed door de scenario's die kunnen worden nagebootst. Het vermogen van de Cyber Range om ontwikkeling van nieuwe scenario's te ondersteunen, door gebruikers of derden, vergroot de waarde van een Cyber Range aanzienlijk. Om deze reden zijn binnen sommige Cyber Ranges hulpmiddelen en tools beschikbaar voor het samenstellen van scenario's. Dit kan variëren van basissimulatie omgevingen tot aangepaste simulaties van aanvallen en andere diensten.

Competency Management: Competentiebeheersystemen kunnen organisaties helpen bij het beheren van hun competentieprogramma's. Hiermee kunnen vaardigheidstekorten geanalyseerd worden, leertrajecten gevormd worden, of competenties mee worden geëvalueerd. Dit stelt organisaties in staat om competenties van werknemers op peil te houden.

Data Collection and Analysis: Dataverzameling is de mate waarin de Cyber Range het mogelijk maakt om gegevens te verzamelen, zoals geheugendumps, netwerkverkeer, of log informatie. Door middel van gegevensanalyse kunnen Cyber Ranges effectief informatie verzamelen en gebruiken om het ontwerp, de werking en het gebruik van de Cyber Range te optimaliseren. Dit kan leiden tot verbeterde leerervaringen, betere prestaties en hogere mate van effectiviteit van de Cyber Range voor verschillende doeleinden.

Scoring and Reporting: biedt een out-of-band methode om de prestaties van gebruikers van een Cyber Range te evalueren op basis van hun activiteiten en interacties met de Cyber Range. Out-of-band is een manier om van buiten het netwerk veranderingen door te kunnen voeren of te monitoren wat de status is van systemen en processen. Rapportage kan dan ook informatie bevatten per gebruiker, of per team, wat het mogelijk maakt voor organisaties om inzicht te krijgen in cybercapaciteiten.

Instructor Tools: biedt functionaliteiten en hulpmiddelen aan instructeurs om een Cyber Range effectief te gebruiken voor onderwijs of opleidingsdoeleinden.



Figuur 3.2: Cyber-Range referentiearchitectuur (ECSO). Uit [2].

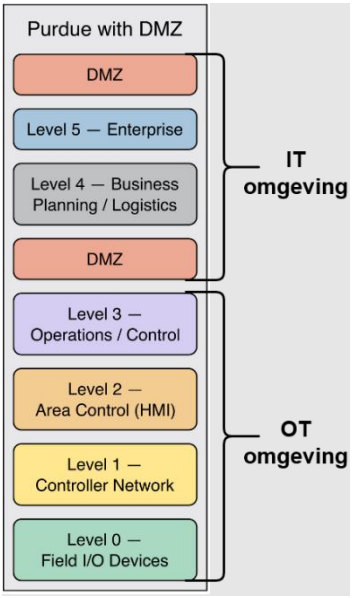
3.3 Cyber Range en (Security) Testbeds

Naast de term Cyber Range is ook de term (Security) Testbed in literatuur en praktijk te vinden. Binnen de literatuur is het verschil tussen een Cyber Range en een Testbed niet altijd even duidelijk en worden de termen Cyber Range, Testbed en Security Testbeds regelmatig door elkaar gebruikt. De eerder genoemde literatuurstudie van Yasim et al. [8] stelt vast dat de termen (security) Testbeds en Cyber Ranges veelvuldig door elkaar worden gebruikt. Terwijl er geobserveerd kan worden dat Ukwandu et al. [9] op basis van een soortgelijke studie stelt dat er wel degelijk verschillen zijn. Het verschil ligt in de aanvalsscenario's die gesimuleerd of geëmuleerd kunnen worden. Zo simuleren Testbeds volgens Ukawandu et al. [9] aanvallen op kritieke infrastructuren, zoals energiecentrales, terwijl Cyber Ranges vaak grotere (IT) netwerk architecturen met verschillende services en applicaties kunnen simuleren. Hierbij wordt het voorbeeld gegeven van een datacentrum, bedrijfsnetwerken, of met het internet verbonden IT/OT-systemen. Cyber Ranges worden vo lgens de onderzoekers met name voor IT-omgevingen toegepast, terwijl Testbeds de voorkeur geniet in OT-omgevingen.

Als er echter uit wordt gegaan van de eerder gestelde definitie van ECSO uit hoofdstuk 3.1, kan er een onderscheid gemaakt worden tussen (Security) Testbeds en Cyber Ranges op basis van het feit dat een Cyber Range een hoge mate van configureerbaarheid omvat, waardoor het eenvoudig is om verschillende omgevingen te creëren. Verder biedt een Cyber Range, in tegenstelling, tot een Testbed een platform voor verschillende gebruiksdoelen (zoals beschreven in hoofdstuk 3.1), en niet alleen voor (cyber)testen.

3.4 IT, OT, ICS en SCADA

Binnen de watersector worden de begrippen Industrial Control System (ICS), Operational Technology (OT) en Supervisory Control and Data Acquisition (SCADA) frequent gebruikt. Om context te creëren voor de toepassing van Cyber Ranges en Digital Twins (binnen de watersector) is het van belang om deze termen kort te bespreken aan de hand van het Purdue referentiemodel, zie figuur 3.3. Dit model geeft een goed overzicht van een algemene IT-omgeving in relatie tot de OT-omgeving verantwoordelijk voor de aansturing van de vitale processen binnen de watersector. Vooral de termen OT en SCADA van dit model zullen dan ook worden gebruikt ter referentie in de rest van dit rapport. Bovendien kan het model worden gebruikt als blauwdruk voor de implementatie van OT-omgevingen en kan het dienen als een leidraad voor de juiste aanpak van een Cyber Range binnen deze sector.



Figuur 3.3: Purdue referentiemodel. Uit [10].

Informatie Technologie (IT) is een brede term die diensten, apparatuur of onderling verbonden systemen omvat, gebruikt voor de automatische verwerving, opslag, manipulatie, beheer, controle, weergave en verzending van gegevens of informatie. Een IT-omgeving omvat typisch computers, netwerken, servers, software en databases, evenals de mensen en processen die deze systemen beheren en ondersteunen [10].

Operationele Technologie (OT) is een overkoepelende term voor de hardware en software die industriële processen uitvoeren, controleren en aansturen. Hoewel de terminologieën OT en ICS enigszins verschillen in hun inhoud, kunnen ze toch als verwant worden beschouwd. OT wordt ook wel aangeduid als Industrial Control System (ICS) [10]. Ter vereenvoudiging wordt de term OT gebruikt in het vervolg van dit rapport. De verantwoordelijkheden van de verschillende lagen in het Purdue model kunnen als volgt worden samengevat:

- **Level 5 & 4** – Enterprise laag & Business planning/logistics laag omvat het niveau met de interne IT-systemen en applicaties die worden gebruikt op bedrijfsniveau. Bijvoorbeeld: Interne mail diensten, databases, Human Resource oplossingen, of documentenopslag.
- **Level 3** – Operationeel beheer betreft de laag waarin productiebesturingssystemen worden gebruikt om het productieproces van de gewenste eindproducten te regelen.

- **Level 2** – Controleapparatuur: Deze laag omvat regelkamerwerkstations en Human Machine Interfaces (HMI).
- **Level 1** – De laag van regelapparatuur omvat intelligente apparatuur, zoals programmeerbare logische controllers (PLC's) en Remote Terminal Units (RTU's).
- **Level 0** – De apparatuur onder controle betreft de fysieke sensoren, actuatoren en andere hardware die directe interactie hebben met het fysieke proces. De productiezone wordt gekenmerkt door componenten die worden gebruikt om fysieke processen te bewaken, controleren en automatiseren, zoals sensoren en actuatoren.

4 Begrippenkader Digital Twin

4.1 Definitie

Evenals voor het begrip Cyber Range is er geen eenduidige definitie voor het begrip Digital Twin. Wel zijn er terugkerende elementen te destilleren uit de verschillende definities. Hieronder is een aantal relevant en vaak geciteerde definities weergegeven. Een terugkerend element in alle definities is dat er een permanente verbinding en voeding is vanuit een fysiek object of proces naar de digitale representatie daarvan. Fysiek en digitaal vormen daarmee dus samen vaak een feedback loop. De doelstellingen van deze feedback loop kunnen, afhankelijke van de toepassing, verschillen.

Technologieconsultant Gartner houdt definities bij van technische concepten, voor Digital Twin geven zij de volgende definitie:

"A Digital Twin is a digital representation of a real-world entity or system. The implementation of a Digital Twin is an encapsulated software object or model that mirrors a unique physical object, process, organization, person or other abstraction. Data from multiple Digital Twins can be aggregated for a composite view across a number of real-world entities, such as a power plant or a city, and their related processes. [11]"

Deze definitie is voornamelijk technisch georiënteerd en richt zicht vooral op het ontwerp en implementatie proces van een Digital Twin, het toepassingsperspectief ontbreekt hier echter. Het internationale Digital Twin Consortium [12], dat zich voornamelijk op standaardisatie-activiteiten en uniformering richt, definieert Digital Twins als volgt:

"A Digital Twin is a virtual representation of real-world entities and processes, synchronized at a specified frequency and fidelity."

Deze definitie voegt een tijdsaspect toe (frequency) en een mate van detail en nauwkeurigheid (fidelity). Daarmee wordt dan ook de link gelegd naar het gebruiksdoel van een Digital Twin. De mate waar in de digitale representatie synchroon loopt (frequentie van update) met het fysieke object en de mate van detail van de virtuele representatie kunnen, afhankelijk van het gebruiksdoel, verschillen.

Aan deze definitie voegt het Digital Twin Consortium een aantal gebruiksperspectieven toe met relevante elementen:

- Digital Twin systems transform business by accelerating holistic understanding, optimal decision-making, and effective action.
- Digital Twins use real-time and historical data to represent the past and present and simulate predicted futures.
- Digital Twins are motivated by outcomes, tailored to use cases, powered by integration, built on data, guided by domain knowledge, and implemented in IT/OT systems.

Deze definitie is completer omdat het de technische aspecten en een toepassingsperspectief schetst. De definitie blijft echter wel generiek en heeft, in het kader van dit rapport, een vertaling nodig naar toepassing binnen de watersector.

Onderzoeksorganisatie van de drinkwaterbedrijven KWR sluit qua definitie aan bij bovenstaande generiekere definities en geeft de toepassingen daarvan aan voor drinkwaterbeheer. Tevens wordt in de definitie de link gelegd naar toepassingen ten behoeve van productieproces-optimalisatie en monitoring van waterkwaliteit (optimalisering van de bedrijfsvoering).

"Een digitale tweeling of Digital Twin is een virtuele kopie of model van de werkelijkheid met een zo goed mogelijke benadering van het fysieke proces. Sensormetingen van de fysieke werkelijkheid worden gevoed aan modellen van de digitale tweeling. Deze datafusie van sensordata en model kan ertoe leiden dat voor niet-(online)meetbare parameters toch een realtime inschatting van hun waarde beschikbaar is. Dit worden virtuele sensors of softsensors genoemd. [13]"

KWR maakt in hun definitie ook nadrukkelijk de combinatie met gebruik van sensortechnologie.

Bij Wageningen University & Research (WUR) loopt een onderzoeksproject rondom Digital Twin voor waterbeheer. De WUR beschrijft het begrip Digital Twin zoals beschreven in hoofdstuk 2.

Vanuit deze definitie beschrijft WUR de toepassing hiervan voor de watersector, waarbij de 'physical twin' het daadwerkelijke gemonitorde watersysteem van de waterschappen is en de Digital Twin de set van geïntegreerde rekenmodellen, (AI-)algoritmen, visualisatiesystemen/dashboards en de structuur die deze verschillende onderdelen verbindt. Een Digital Twin voor waterbeheer betekent dus een verdere integratie en gebruik van data, modellen, workflows en de implementatie daarvan in de complexe operationele processen.

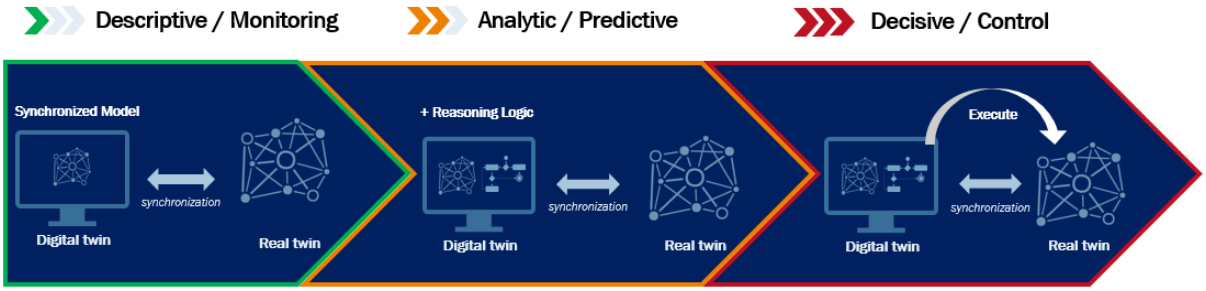
Voor het doel van dit rapport sluiten we aan bij de definitie die WUR heeft beschreven. Het omvat de meest belangrijke functies van een Digital Twin, sluit aan bij de generiekere definities en sluit aan bij toepassingen in de watersector.

4.2 Toepassingsperspectieven Digital Twins

Zoals ook uit de verschillende definities van Digital Twins blijkt, worden ze voor verschillende doeleinden gebruikt. Soms ligt de focus meer op monitoring van huidige gebeurtenissen om deze te vergelijken met data van normaal gedrag uit het verleden, aan de andere kant van het spectrum zitten Digital Twins met meer voorspellende karakter. In de literatuur worden Digital Twins daarom ook vaak in 3 categorieën in gedeeld:

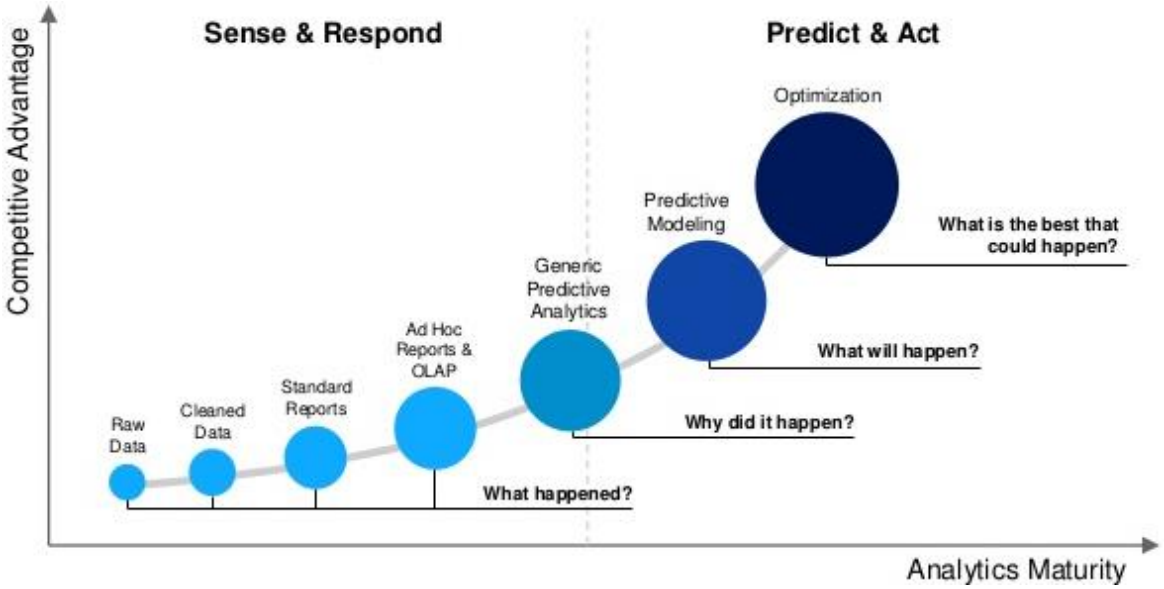
1. ***Reactive Digital Twin**:* dergelijke Digitale Twins helpen om de activiteiten en processen van de watersector te bewaken en de gebruikers te waarschuwen als er iets afwijkt van het verwachte gedrag.
2. ***Predictive Digital Twin**:* deze Digital Twin maakt het mogelijk om "wat-als"-scenario's uit te voeren en voorspellingen te doen voor de benodigde waterkwaliteit en correcte waterlogistiek voor de toekomst.
3. ***Prescriptive Digital Twin**:* de Digital Twin die in staat is om de fysieke entiteit daadwerkelijk te besturen door de commando's terug te sturen naar het fysieke systeem

om specifieke bewerkingen uit te voeren, waardoor de prestaties of de algemene werking van het systeem kunnen worden gewijzigd.



Figuur 4.1: Evolutie van Digital Twin gebruik: Van Bewaking over het fysieke systeem tot controle over complexe systemen. Uit [14].

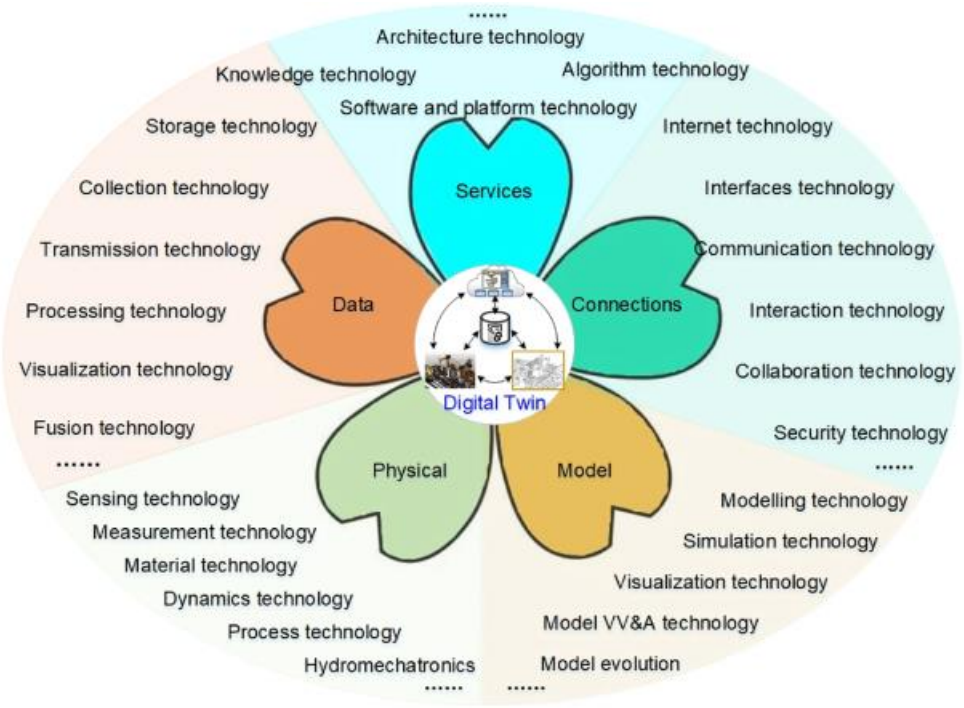
Zodra processen digitaal zijn getransformeerd en infrastructuren zijn uitgerust met sensoren en er dus veel data beschikbaar komt, is de volgende logische stap om waarde uit al deze data te halen. Naast het simuleren van scenario's voor betere besluitvorming, helpen Digital Twins ook bij het testen van veranderingen in operationele processen. Een groeipad naar steeds geavanceerdere data analyse sluit daarom goed aan bij een groeimodel van Gartner op dit gebied, zoals hier onder weergegeven in figuur 4.2.



Figuur 4.2: Gartner's maturiteitsmodel voor data-analyse. Uit [11].

4.3 Hoofdelementen Digital Twin

De literatuur over Digital Twins beschrijft vaak de belangrijkste aspecten en componenten die een rol spelen in de realisering van Digital Twins. In [14] wordt een vijf-dimensioneel model voor Digital Twins beschreven (figuur 4.3), die feitelijk een verdiepende uitwerking is van de elementen die in de definitie (zie paragraaf 4.1) zijn benoemd.



Figuur 4.3: Vijf-dimensioneel model voor het beschrijven van componenten en enabling technologies van Digital Twins. Uit [14].

De vijf dimensies zijn (1) fysieke entiteiten, (2) virtuele modellen, (3) data, (4) services, en (5) connecties. Deze dimensies worden ondersteund door zogenaamde 'enabling technologies', oftewel technologieën die de verschillende dimensies van Digital Twins mogelijk maken en ondersteunen. Hieronder worden de vijf dimensies en enabling technologies kort samengevat.

1. Fysieke entiteiten

De fysieke entiteit is de basis van de Digital Twin, en kan een product, een fysiek systeem, proces of organisatie zijn. Enabling technologies zijn de middelen die gebruikt worden om de entiteit te begrijpen en te beschrijven, zoals metingen en data analyse, en de middelen die gebruikt worden om de entiteit te sturen, zoals control systems.

2. Virtuele modellen

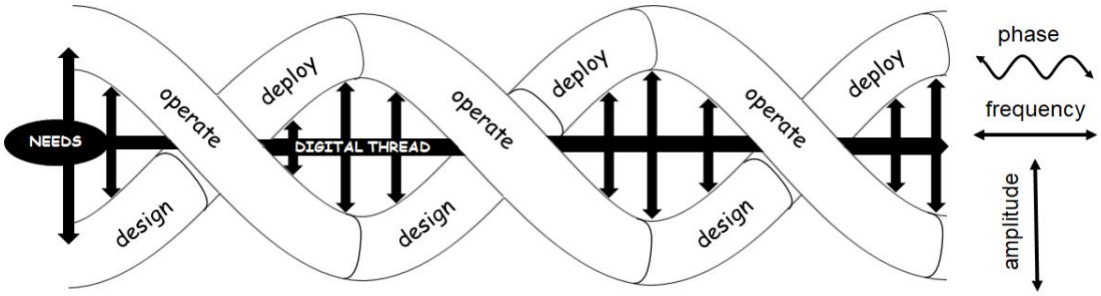
Deze dimensie omvat de modellering van de fysieke entiteiten die de Digital Twin behelst. Uiteindelijk is het idee van de Digital Twin een real-world entiteit zo goed mogelijk na te bootsen, en de mate waarin dit lukt is sterk afhankelijk van de kwaliteit van de modellen die gebruikt worden. Voorbeelden van enabling technologies zijn bijvoorbeeld geometrisch en mechanistisch modelleren, parameterisering en data-gedreven modelleertechnieken, waaronder machine learning.

3. Data
Interactie met data is één van de belangrijkste principes van de Digital Twin. Data in Digital Twins kunnen komen van de fysieke entiteit, het virtuele model, de omgeving, kennis en gerelateerde services. Dat kan statisch of dynamisch zijn. De interacties worden mogelijk gemaakt door (verbeterde) datatransmissie-technologie, dataopslag, dataprocessing, data-fusion (samenbrengen en combineren van verschillende soorten data) en datavisualisatie.

4. Services
Een ander essentieel aspect is het aanleveren van de functionaliteiten van de Digital Twin als 'services', aangezwengeld door de Everything-as-a-service paradigma (XaaS). Dit houdt bijvoorbeeld in de simulatieomgeving die aan de gebruiker wordt aangeboden als platform service, maar het kan ook andere functionaliteit of externe services betreffen.

5. Connecties
Connecties in Digital Twins zijn essentieel voor het uitwisselen van data en informatie. De connecties kunnen bestaan tussen de fysieke entiteit, het virtuele model, services en data. Technologie die hierin een rol speelt bestaat onder andere uit real-time technologie en draadloze netwerken, maar ook de protocollen en de beveiligingsmethoden die daarbij horen.

Digital Twins zijn als replica van veelal complexe systemen gevoelig voor de dynamica die in het fysieke systeem plaatsvinden. Hierdoor gaat de *lifecycle management* van een Digital Twin verder dan typisch het geval is bij systeem engineering. De belangrijkste uitdaging bij Digital Twins van complexe, dynamische systemen is hoe het onderhoud en het operationele deel van de twin tegelijkertijd beheerd kan worden. In [15] worden ideeën uit de systeem engineering en IT toegepast om tot een lifecycle model voor Digital Twins te komen. Het resultaat is het 'double helix' model (zie figuur 4.4) voor lifecycle management van Digital Twins.



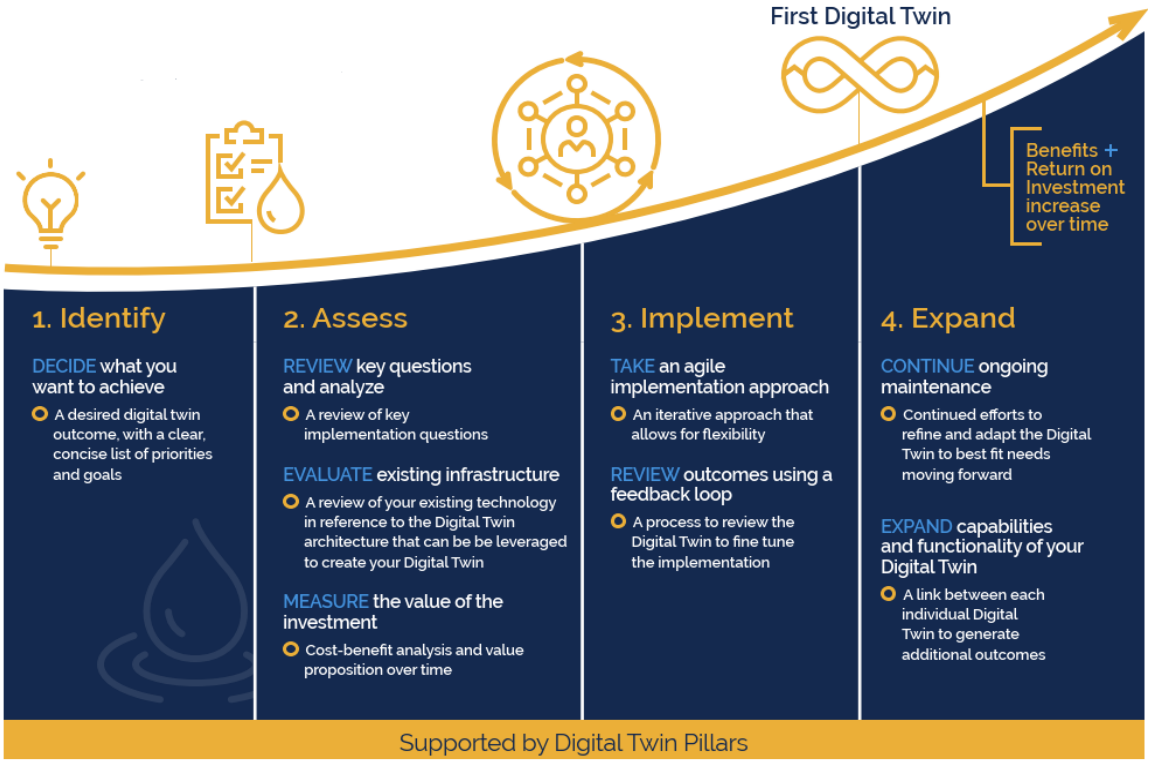
Figuur 4.4: Double Helix model voor DT lifecycle management. Uit [15].

In het double helix model komen het einde van de deployment (het in implementeren en in werking brengen) stages samen met de operationele fase van de andere lijn. Dit houdt in dat de nieuwe versie van de Digital Twin operationeel komt op het moment dat de huidige vervangen moet worden. Afhankelijk van de precieze context van de Digital Twin, kan de double helix anders worden weergegeven. Drie aspecten die van belang zijn voor Digital Twins komen terug in de karakteristiek van de double helix, namelijk:

- Omgevingsdynamiek (frequentie): Hoe groter de dynamiek is in de omgeving waarin de twin opereert, hoe hoger de frequentie van cycli is.
- Systeemcomplexiteit: Bij een complexer system zijn de uitdagingen wat betreft modelleren, integreren en configureren van componenten groter.

- Leidende twin: Afhankelijk van de situatie en de stage in het Digital Twin proces is de Digital Twin of de Physical Twin leidend. Wanneer de Digital Twin leidend is, dan wordt deze gebruikt om de doelen van het system te behalen. Wanneer de fysieke twin leidend is, dan wordt deze gebruikt voor de ontwikkeling van de nieuwe Digital Twin. In veel situaties zullen deze fases afwisselen.

Afhankelijk van de toepassing en de complexiteit van de entiteit waar de Digital Twin betrekking op heeft, bestaat de ontwikkeling uit verschillende fases. Bij complexe operationele doelen, is het de ontwikkeling vaak een iteratief proces. De SWAN (Smart Water Networks Forum) werkgroep voor Digital Twins heeft een schaalbare en flexibele handleiding gemaakt voor het ontwikkelen van Digital Twins (zie figuur 4.5). Het proces start met het *beslissen* want men wil bereiken met de Digital Twin. Vervolgens moeten sleutelvragen worden *beantwoord,* bestaande infrastructuren worden *geëvalueerd* en de waarde van de investering worden *gemeten.* De implementatiefase bestaat uit een agile *uitvoering* van de taken met betrekking tot de implementatie, waarbij er een feedback loop is om de uitkomsten te *evalueren.* Tenslotte kan de digital worden *onderhouden* en eventueel worden *uitgebreid* [16].



Figuur 4.5: Stappen in het Digital Twin ontwikkelproces. Uit [16].

5 Cyber Ranges en Digital Twins in de watersector en andere sectoren

In dit hoofdstuk zijn voorbeelden van praktische toepassingen van Cyber Ranges en Digital Twins in de watersector en in andere sectoren beschreven.

5.1 Cyber Ranges in de watersector

Het Secure Water Treatment (SWaT) testbed de Singapore University of Technology and Design (SUTD) [17] biedt een moderne ICS-omgeving van zes individuele waterbehandelingsprocessen die achtereenvolgens worden doorlopen. Elk proces wordt bestuurd door de ICS-omgeving. De architectuur vertegenwoordigt een verkleinde versie van een moderne waterzuiveringsinstallatie op ongeveer 90 vierkante meter (zie figuur 5.1). De controlearchitectuur is nauwkeurig afgeleid van een echte waterzuiveringsinstallatie zodat de opstelling zo accuraat mogelijk is. De open omgeving werd initieel gebruikt als testbed, om een platform te bieden voor onderzoek naar cyberbeveiliging in OT-omgevingen (besproken in hoofdstuk 3.4), onderzoek naar detectiealgoritmen, beoordelen van cybersecurity protectiemechanisme, en om inzicht te krijgen naar cascade-effecten binnen operationele omgevingen. Naast de testbedconfiguratie die is ontwikkeld voor specifieke doeleinden, kan de omgeving ook worden ingezet worden als een Cyber Range-configuratie, waarbij het door toevoegen van additionele componenten andere use-cases kan ondersteunen voor bijvoorbeeld het ondersteunen van securityonderzoek, het ontwikkelen van cybercapaciteiten voor personeel door middel van een trainingsomgeving, of mogelijk maken van cybersecurity-competities.

Naast SWaT heeft de universiteit ook WADI ontwikkeld, een fysieke uitbreiding van het eerder beschreven SWaT testbed, dat een waterdistributiesysteem vertegenwoordigt (figuur 5.2). WADI kan worden gebruikt om inzicht te krijgen in cyberaanvallen die fysieke schade veroorzaken op grootschalige waterdistributiesystemen en de cascade-effecten die daaruit voortvloeien [18]. Het Wadi testbed bestaat uit drie achtereenvolgende processen die evenals het SWaT testbed worden bestuurd via een ICS-controle architectuur. Het testbed is fysiek verbonden met het SWaT testbed om gefilterd water te ontvangen en te “distribueren”.

Doordat SWaT en WADI unieke posities hebben in de academische wereld vormt de data afkomstig uit deze testbeds de basis voor veel wetenschappelijke publicaties naar aanvalsdetectie in industriële control systemen [19, 20].

Het derde door Itrust SUTD geïntroduceerde testbed is het Electrical Power and Intelligent Control (EPIC) testbed. Het is een representatie van micro-elektriciteitsopwekkings-architectuur voor de opwekking en distributie van elektriciteit [21] . Ondanks dat het EPIC testbed geen water gerelateerde Cyber Range is, kunnen dergelijke specifieke omgevingen

ook worden ingezet in een Cyber Range-configuratie waarbij zowel, SWaT, WADI, en EPIC worden gecombineerd voor grootschalige cyberoefeningen en trainingen. Het Critical Infrastructure Defence Exercise (CIDeX 2022) [22, 23] of de meer recente CISS 2023 [24] zijn voorbeeld en van grote hands-on oefeningen voor de verdediging van operationele technologie in kritieke infrastructuren. Meer dan 17 verschillende organisaties uit diverse sectoren, waaronder water, telecom, transport en maritieme, hebben deelgenomen aan deze oefening aan de hand van de drie aaneengesloten testbeds die samen een grootschalige kritieke infrastructuuromgeving nabootsen. Deze voorbeelden laten goed zien dat testbedden en Cyber Ranges vaak een hoge mate van configureerbaarheid hebben en ook vaak kunnen bestaan uit een combinatie van technologieën, volledig virtueel, hybride of volledig fysiek, die met elkaar kunnen worden gekoppeld voor een bepaald doel.

Giuliano en Formicola [25] introduceren met hun onderzoek: *ICSRange - A Simulation-based Cyber Range Platfrom for Industrial Control systems een* proof-of-concept voor een ICS Cyber Range met een gesimuleerd fysiek waterprocessen en SCADA-systeem. De Cyber Range emuleert (volledig virtueel) een deel van een IT-omgeving en een OT-omgeving. In de omgeving kan een aanval worden gesimuleerd, bestaande uit meerdere fasen waarbij de OT-omgeving geleidelijk wordt binnengedrongen en de waterprocessen worden aangevallen. De auteurs geven aan dat de Cyber Range gebruikt kan worden voor teambuilding, onderzoek, ontwikkeling, het testen en beoordelen van cybersecurity-maatregelen, en ten slotte, capture-the-flags waarbij cybersecurity puzzels of challenges opgelost moeten worden.

De Verenigde Staten beschikken over een Water Security Test Bed (WSTB). Het WSTB is gebouwd op het Idaho National Laboratory (INL) en bevat een replica van een deel van een gemeentelijk drinkwatersysteem [26]. Van oorsprong richtte dit testbed zich op een aantal fysieke security risico's (zoals chemische besmetting). Recent wordt het testbed ook gebruikt voor cyberrisico's. Het testbed wordt bijvoorbeeld benut om kwetsbaarheden en maatregelen uit te testen binnen de OT-omgeving van een typisch watersysteem.

Figuur 5.1: SWaT testbed. Uit [74].

Figuur 5.2: Wadi testbed. Uit [75].

5.2 Digital Twins in de watersector

Digital Twins bieden meerdere voordelen voor de watersector. Door verschillende scenario's te simuleren, waaronder noodsituaties, gezondheidswaarschuwingen en aan klimaatverandering gerelateerde gebeurtenissen, kunnen Digital Twins een organisatie helpen potentiële problemen beter te anticiperen en flexibeler te reageren, waardoor risico's, tijd en kosten worden verminderd.

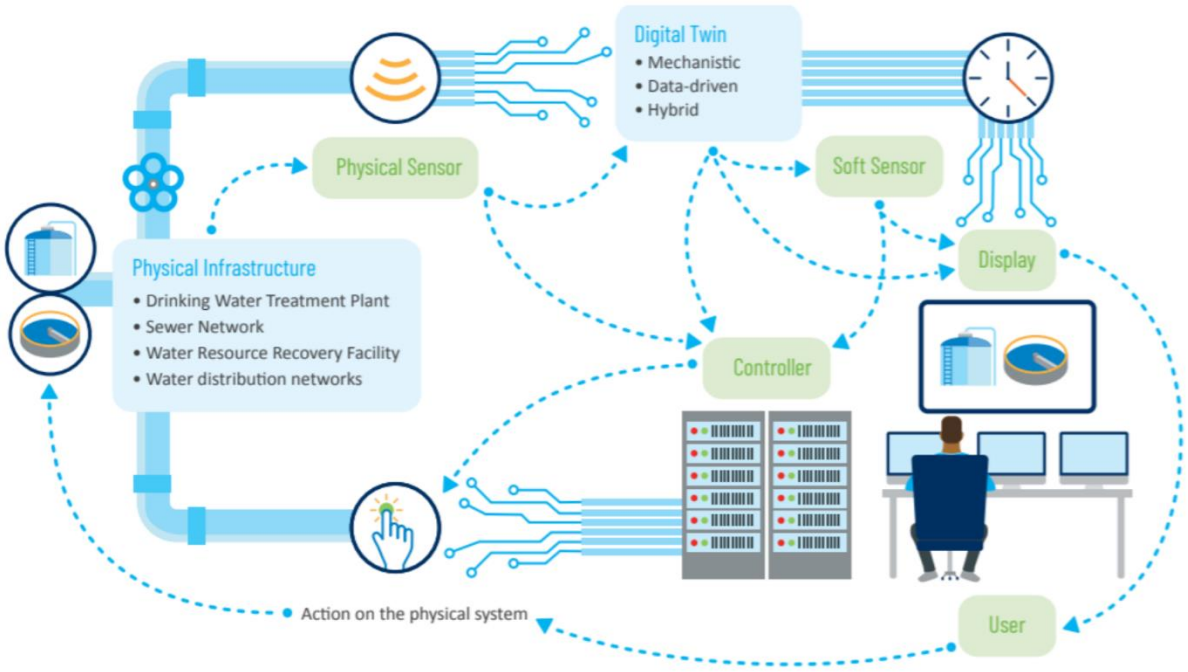
Daarnaast kunnen Digital Twins helpen de efficiëntie te verhogen door de systemen in een organisatie te optimaliseren. Bovendien kunnen ze klantgericht beheer verbeteren. Naarmate een organisatie beter in staat is om op potentiële problemen te anticiperen en respons plannen te formuleren, vermindert het de verstoring van de dienstverlening aan haar klanten. Ten slotte kunnen Digital Twins helpen om niet alleen systemen, maar ook grotere infrastructuren duurzamer en veerkrachtiger te maken in hun reactie op klimaatverandering door middel van planning, optimaal infrastructuurbeheer en burgerparticipatie.

In een huis kan een Digital Twin waterlekkage helpen verminderen. In een stad kan een Digital Twin helpen bij het monitoren van inkomende overstromingen. Op een boerderij kan een Digital Twin landarbeiders helpen water efficiënter te gebruiken om mogelijke droogte aan te pakken. Ten slotte kan een Digital Twin steden en industrieën helpen de waterkwaliteit te behouden door de verontreinigingen of verontreinigende stoffen in afvalwater te meten.

De succesvolle inzet van Digital Twins zal de komende jaren echter van bedrijven in de watersector vergen dat zij een aantal uitdagingen overwinnen. Deze uitdagingen zijn onder meer te vinden in de datakwaliteit, de locatie van externe systemen waardoor ze moeilijk te verbinden zijn, en de noodzaak om een simulatiemodel up-to-date en in real time operationeel te houden.

In [27] wordt het idee en gebruik van Digital Twins in de stedelijke watersector gereviewed. Duidelijk wordt dat, tegelijk met de toename van het aantal publicaties over Digital Twins, ook het aantal artikelen dat gaat over Digital Twins in de watersector toeneemt. Toenemende interesse in Digital Twins in de watersector wordt ook duidelijk uit de verschillende workshops en white papers van verschillende waterorganisaties, zoals SWAN (Smart Water Networks Forum) en IWA (International Water Association).

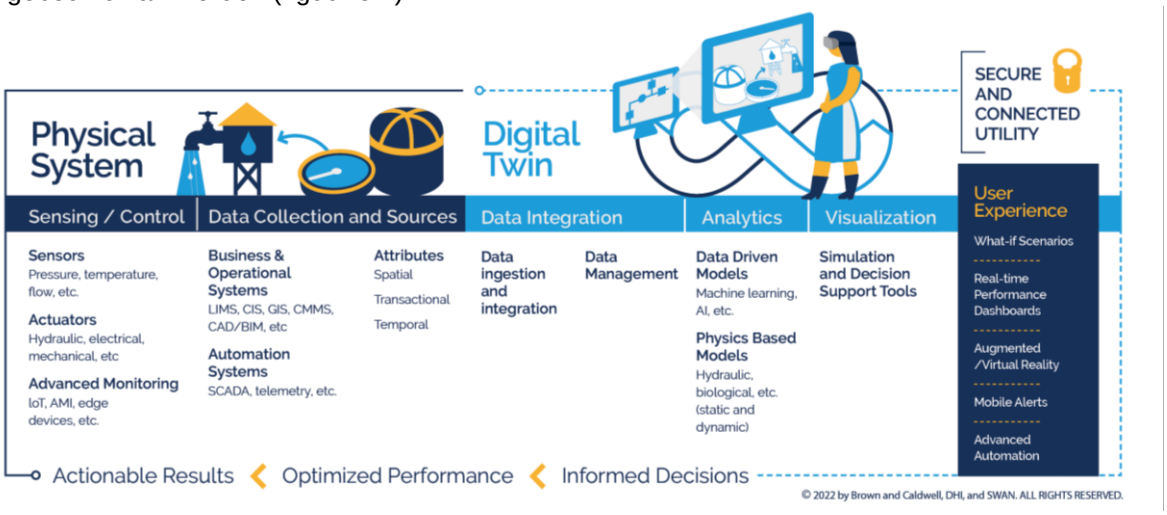
IWA (International Water Association) publiceerde in 2019 het rapport “Digital Water” [28]. In dit rapport wordt Digital Twin-technologie als een van de ‘transformative digital solutions’ genoemd voor digital water en afvalwater management, en omschreven als “Data integration, analytics, and visualisation capabilites to help utility managers gain control of the intelligent systems they’ve deployed”. Digital Twins worden herkend als een middel om bijvoorbeeld meer accurate beslissingen, efficiëntere processing, betere interactie met gebruikers en stakeholders, en meer weerbaarheid tegen veranderende omstandigheden. In figuur 5.3 wordt de basisstructuur, volgens IWA, van een Digital Twin voor water getoond.



Figuur 5.3: Basisstructuur van Digital Twin in de watersector. Uit [71].

Het SWAN (Smart Water Networks Forum) heeft sinds 2019 een *Digital Twin Utility Advisory Group* dat zich richt op het ontwikkelen van een Digital Twin strategie en implementatie in de watersector. De groep richt zich op met name holistische architectuur, Digital Twin lifecycle, BIM & Asset management, en uitkomsten en toepassingen. De werkgroep heeft in de loop der tijd een Digital Twin architectuur ontwikkeld, zoals te zien is in figuur 5.4.

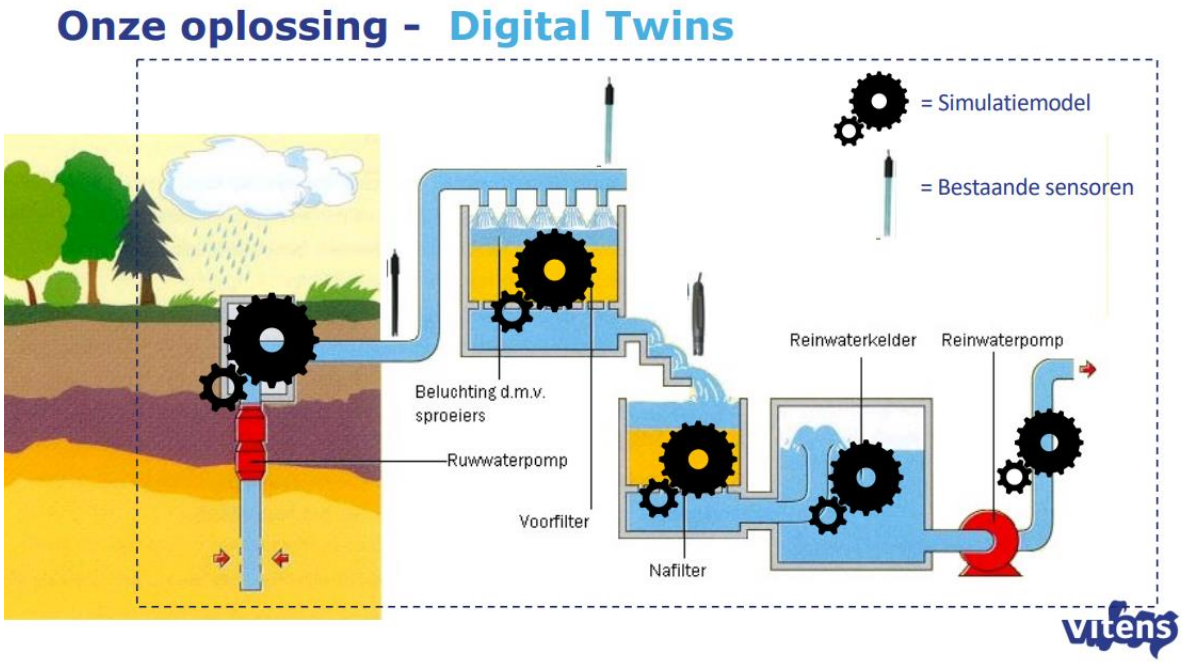
Ook heeft de werkgroep een *Digital Twin Readiness Guide* [16] gepubliceerd, waarin wordt beschreven wat Digital Twin zijn, use cases worden beschreven en hoe een Digital Twin gebouwd kan worden (figuur 5.4).



Figuur 5.4: SWAN Digital Twin architectuur. Uit [16].

5.2.1 Vitens

Drinkwaterbedrijf Vitens maakt gebruik van een digital twin toepassing. Vitens wil hiermee de productielocaties, de distributiesystemen en -netwerken monitoren en controleren. De achterliggende vraag is hoe de efficiëntie in de productie en distributie op dit moment is en hoe deze te verbeteren is [76].

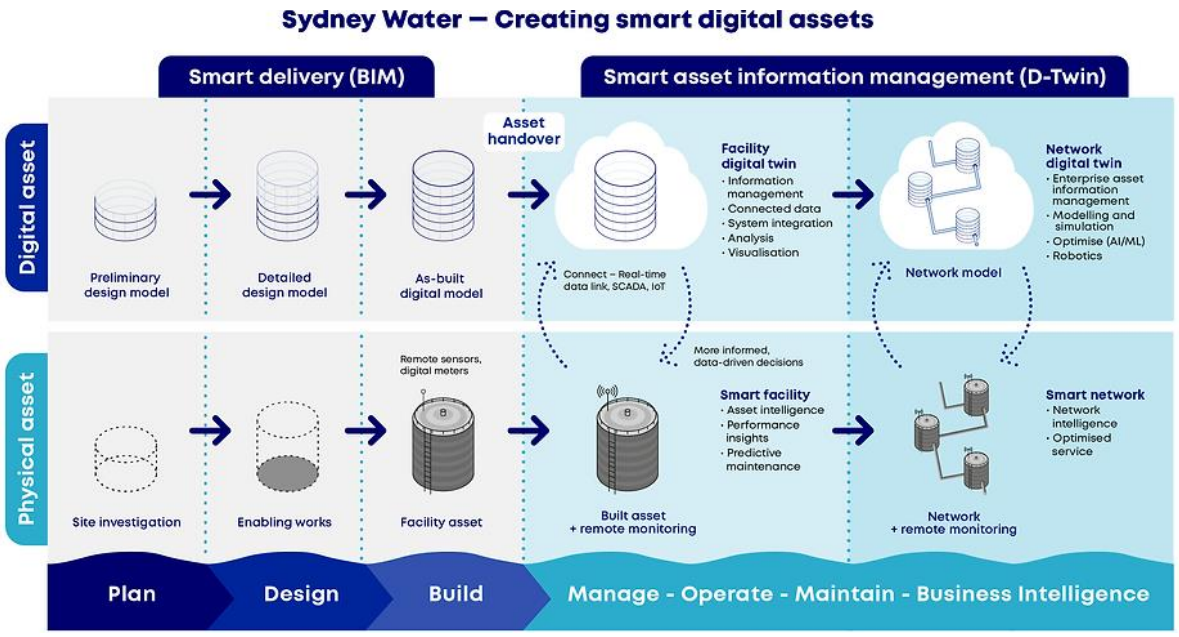


Figuur 5.5: Digital Twins bij Vitens. Uit [77].

Vier jaar geleden constateerde Vitens dat de distributiepompen bij een van haar drinkwaterproductiebedrijven verre van optimaal functioneerden. Aanpassingen doorvoeren in de oude softwarebesturing vormde een riskante onderneming [76]. Vandaar dat voor diagnose een simulatie van de bestaande situatie van de pompopstelling werd gedaan. Uiteindelijk werden de ideale pompconfiguratie en aansturing van de pompen bepaald. De simulatie werd op wens van Vitens direct uitgebreid om ook inzicht in energieverbruik te geven. Het resultaat: goed werkende pompen en met brondata van Vitens inzicht in energiebesparing en voorspelbaar onderhoud. Vitens was meer dan voorheen ‘in control’ en de simulatie is nu een van ‘Digital Twins’ om nieuwe scenario’s te testen (zie figuur 5.5).

5.2.2 Sydney Water

Sydney Water gebruikt een digitaal raamwerk om de manier te verbeteren waarop hun bedrijfsmiddelen worden gepland, ontworpen, gebouwd, geëxploiteerd en onderhouden gedurende hun hele levenscyclus (zie figuur 5.6).



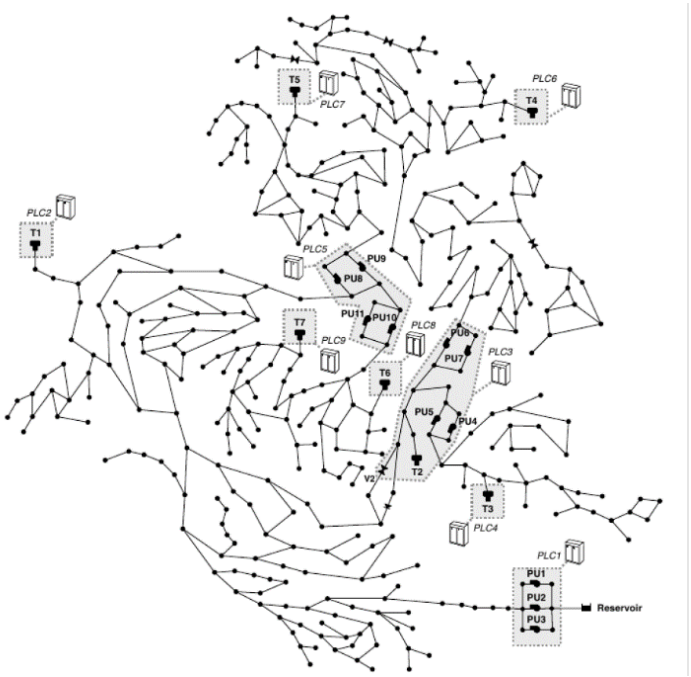
Figuur 5.6: Digital Twins in Sydney Water. Uit [78].

Het doel van de Digital Twin van Sydney Water in de toekomst zal zijn om beslissingen over vermogensbeheer te automatiseren. Het plan voor Digital Twins is om project-informatiemodellen te ontwikkelen. In het eerste jaar zijn de experts aan het standaardiseren, wat betekent slim, virtueel digitaal vermogensbeheer en -creatie. Het tweede jaar gaan ze in op samenwerking. Ze introduceren nieuwe technologieën, coördinatiepraktijken en verbeterde projectprestaties. Het volgende jaar gaat over integratie. Het gaat om het bedenken van een gemeenschappelijke data-omgeving, het opzetten van nieuwe processen en het beheren van de informatie via nieuwe technologieën en platforms. Het komende jaar zal in het teken staan van visualisatie, gericht op nieuwe manieren van werken, real-time prestatiestatistieken en modellering. Het laatste jaar gaat over optimalisatie, dat gaat over automatisering, simulatie, analyse, machine learning en een op inzichten gebaseerde aanpak [78].

5.2.3 Digital Twin voor de cyberveiligheid van drinkwaterleidingen

Murillo et al. [29] presenteren in hun paper *Co-Simulating Physical Processes and Network Data for High-Fidelity Cyber-Security Experiments* de tool Digital Hydraulic Simulator (DHALSIM) een open-source Digital Twin van een drinkwater distributie system dat gebruikt kan worden voor cyberdoeleinden. De tool maakt gebruikt van een combinatie van een water distributie Digital Twin en OT-emulator om een OT aangestuurde drinkwaterinstallatie na te bootsen. Dit stelt cybersecurity-onderzoekers in staat om 'willekeurige' waterdistributie systemen en OT-netwerkarchitecturen in te zetten, waarbij het mogelijk wordt om een breed scala aan omstandigheden te simuleren.

Bovendien biedt de Digital Twin de mogelijkheid om ingebouwde aanvalsscenario's af te spelen, afhankelijk van de gekozen configuratie (zoals de mogelijke architectuur in figuur 5.7). Ook kunnen er door middel van de omgeving datasets worden gegenereerd, die vervolgens opnieuw kunnen worden gebruikt voor onderzoek naar aanvalsdetectie. Deze eigenschappen maken de Digital Twin tot een relatief voordelige en efficiënte tool voor cybersecurity-onderzoek naar cyberaanvallen op waterdistributie systemen.



Figuur 5.7: C-town, een van de verschillende water distributie netwerken die binnen DHALSIM gesimuleerd kunnen worden. Uit [73].

5.2.4 Digital Twins voor waterkeringen

Als gevolg van klimaatverandering, bodemdaling en toenemende economische waarde van polders zal Nederland de komende jaren fors moeten investeren om het overstromingsrisico op een acceptabel niveau te houden. Door klimaatverandering zal de komende jaren de zeespiegel stijgen en zullen piekafvoeren in stroomgebieden toenemen. Bij waterschappen is er dan ook een groeiende behoefte aan nieuwe methoden voor het permanent en objectief real-time meten, monitoren en beheersen van de verschillende parameters van waterkeringen.

Sinds 2007 zijn verschillende waterschappen, STOWA en Informatiehuiswater aan het experimenteren met digitale dijkbewaking middels in situ - en remote monitoring en het maken van Digital Twin van fysieke waterkeringen.

In 2007 opende de Staatssecretaris van Verkeer en Waterstaat (destijds Tineke Huizinga) de IJkdijk (zie figuur 5.8) [30] [31]. De IJkdijk is een initiatief van TNO, NOM, STOWA (kenniscentrum voor de waterschappen) en Deltares. De IJkdijk is een nagebootste dijk van ongeveer 1 kilometer lang, die volledig is uitgerust met ICT- en sensortechnologie. Het doel van dit project is om te komen tot een efficiëntere beheersing van waterkeringen en uiteindelijk tot een real-time monitoringsysteem voor dijken. Een breed consortium van deelnemers uit het bedrijfsleven, kennisinstellingen en waterbeheerorganisaties deed onderzoek doen naar de praktische toepassing van sensortechnologie in het waterbeheer.

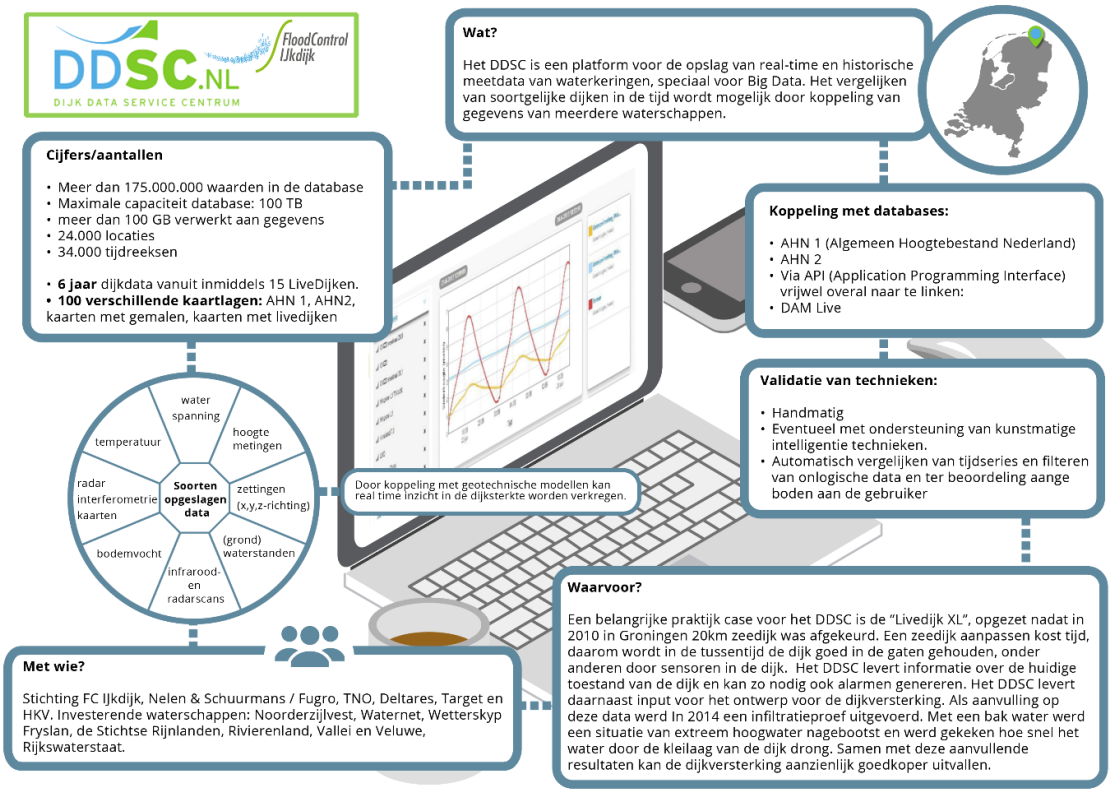
Bij de start van de Ijkdijk en livedijk experimenten was het begrip van “Digital Twin” nog niet geïntroduceerd maar voldoet, met de huidige definitie, hier zeker aan. De ijkdijk heeft dan ook in het kader van Digital Twinning de nodige recente vervolgen geïnitieerd, o.a. [32], [33] en [34].

Bij het beheer van fysieke assets (bijv. waterkeringen) wordt vaak de termen “Data gedreven assetmanagement” en “Digital Twins” nauw aan elkaar verbonden. Rijkswaterstaat formuleert zijn ambities als volgt [35]:

“In 2030 alle assets als real-time Digital Twin verbonden met interne en externe databronnen en modellen. Dit moet ervoor zorgen dat Rijkswaterstaat een integrale benaderingswijze heeft voor het maken van afwegingen waarbij de objectenomgeving en klimaatverandering wordt meegenomen. Hiervoor is behoefte aan een visueel toegankelijke manier om informatie met elkaar te verbinden.”

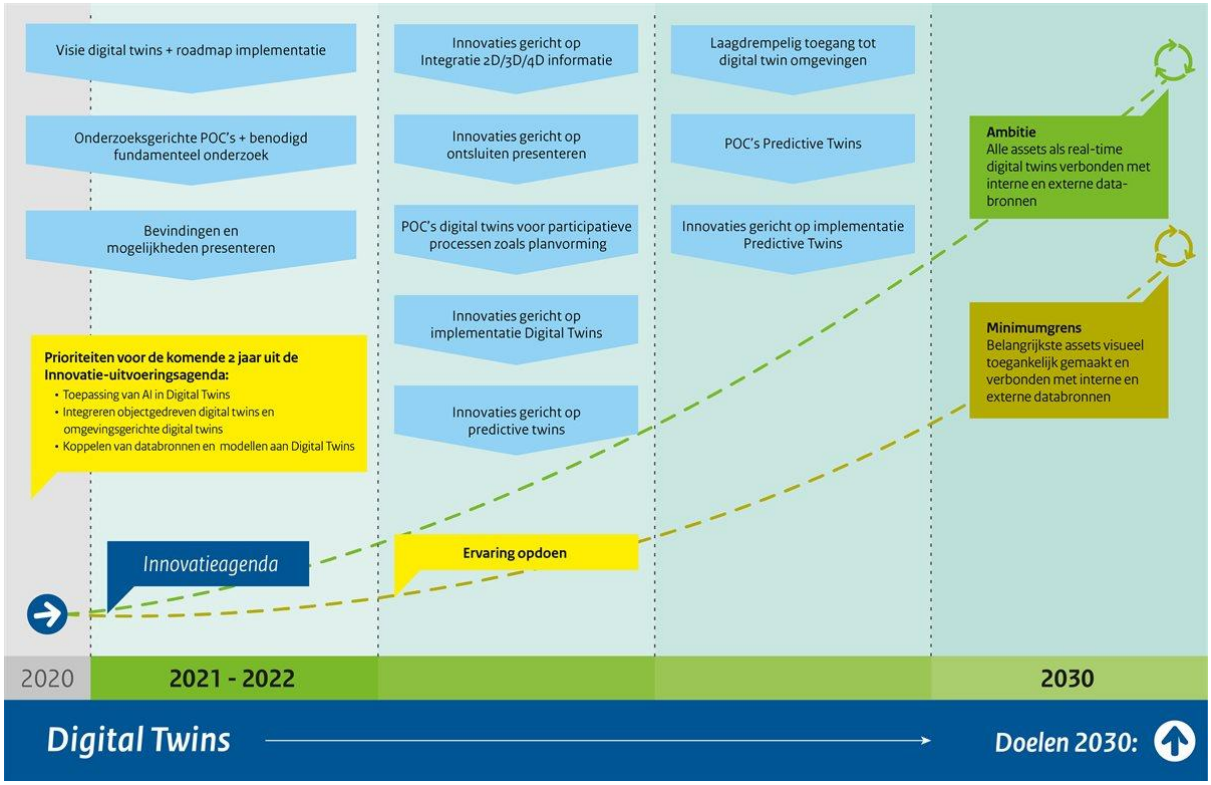
Figuur 5.8: De IJkdijk. Uit [36].

Na een aantal experimenten op beperkte schaal is de stap gemaakt om de technologie toe te passen in operationele dijken, “livedijken” genoemd [37] en is in 2013 het “Dijk Data Service Centrum”(DDSC) operationeel gekomen. Het DDSC is een portal om monitoringsinformatie te verzamelen, op te slaan en beschikbaar te maken voor verdere verwerking (zie figuur 5.9).



Figuur 5.9: Inwinning en ontsluiting van data en informatie. Uit [38].

Bij bovenstaande ambitie van RWS is een roadmap voor Digital Twinning geschetst (figuur 5.10).



Figuur 5.10: Roadmap voor Digital Twins van Rijkswaterstaat. Uit [35].

5.2.5 Overige Use Cases

In [16] worden nog 10 andere use cases van bestaande Digital Twins in de watersector beschreven. Deze use cases zijn samengevat in tabel 5.1. Opvallend is de verscheidenheid aan doelstellingen en scopes van de use cases.

Tabel 5.1: Digital Twin toepassingen in de watersector zoals beschreven in [16].

Naam	Land	Doel	Scope
Tarragona Water Consortium	Spanje	Verminderen electriciteitskosten van het watertransport naar klanten	Volledige waterverzamel- en aanleveringssysteem
Valencia Metropolitan Area	Spanje	Beter beheer van het systeem mbt uitdagingen als bevolkingsgroei, droogte en infrastructuur.	Leidingen, sturingselementen (pompen, kleppen, tanks)
Romagna Acque Società delle Fonti	Italië	Reduceren van de duur van lekkages en verminderen waterverliezen.	Volledige scope van het watersysteem
BlueKolding	Denemarken	Verminderen milieu impact en betere service naar klanten	Volledige water systeem
Gruppo CAP	Italië	Testen en evalueren van operationele keuzes	Waterproductiesysteem
Waterschapsbedrijf Limburg	Nederland	Real-time operationeel management van afvalwatervervoer en -behandeling	Leidingnetwerk en zuiveringsinstallaties voor afvoerwater

Naam	Land	Doel	Scope
PUB, Singapore's National Water Agency	Singapore	Verbeteren afvalwaterzuivering, operationele stabiliteit, productie en service	Volledig systeem
BIOFOS	Denemarken	Optimaliseren van de inzet van de beschikbare capaciteit van het drainage systeem	Kopenhagen's drainagesysteem
VCS	Denemarken	Verbeterd begrip van het systeem, verbeterde planning	Stedelijk drainagesysteem
Kempner Water Supply Corporation	Verenigde Staten	Verhogen efficiëntie van pompstations onder dynamische omstandigheden	Pompinstallaties

5.3 Cyber Ranges in andere Sectoren

Naast Cyber Ranges in de watersector zijn ook andere toepassingsgebieden mogelijk waar Cyber Ranges kunnen worden ingezet.
Chouliaras et al. [39] hebben op basis van een grondige literatuurstudie in hun publicatie: Cyber Ranges and TestBeds for Education, Training and Research verschillende toepassingen van Cyber Ranges geïdentificeerd in vijf verschillende domeinen: defensie, overheid, academische wereld, industrie en private organisaties. Hierbij heeft de publicatie gekeken naar 25 verschillende Cyber Ranges binnen de verschillende genoemde contexten.
Ukwandu et al. [9] zien in hun publicatie: A Review of Cyber-Ranges and Testbeds: Current and Future Trends Cyber Ranges vergelijkbaar met Chouliaras et al. [39] de volgende domeinen waar Cyber Ranges voornamelijk worden toegepast: defensie, inlichtingendiensten en overheid, ondernemingen en commerciële doeleinden en academische toepassingen. In het vervolg van deze sectie zullen we verschillende voorbeelden geven.

5.3.1 Cyber Ranges voor Defensie

NATO Cyber Range
NATO Cyber Range [40, 41] is een belangrijk onderdeel van de NAVO's cyber defensie programma. Het stelt de verschillende bondgenoten instaat om hun cyber-capaciteiten te testen, te oefenen, en op te bouwen. Daarnaast, kan er getraind worden op nieuwe concepten, nieuwe cyberdreigingen en verschillende scenario's iets wat van belang is voor behoud van cybercapaciteiten. De nadruk ligt op het gebruik van realistische scenario's, geavanceerde technologieën, en het simuleren van grootschalige cyberincidenten. De publieke bekendheid van deze Cyber Range, is er een gebrek aan inhoudelijke en technische informatie beschikbaar over deze faciliteit.

5.3.2 Cyber Ranges voor Vitale Infrastructuur

Control Room of the future (TU Delft)
Door de toenemende cyberdreigingen en verdere digitalisering van het elektriciteitsnet heeft TU Delft een nieuw onderzoeksfaciliteit ontwikkeld specifiek voor (cyber)onderzoek naar het "slimme" elektriciteitsnet [42]. De omgeving genaamd: Control Room of The Future is een combinatie van real-time Digital Twin (zie figuur 5.11en figuur 5.12) van een elektriciteitsnet, hardware-in-the-loop die aan de Digital Twin gehangen kan worden en een control room bestaande uit verschillende hard- en software oplossingen van industriële fabrikanten.

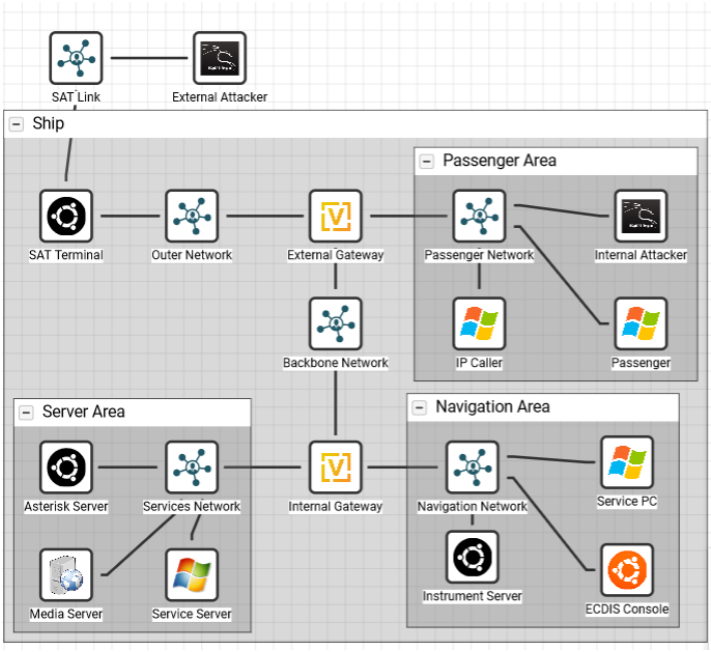
Figuur 5.11: Control Room of The Future. Uit [42].

Figuur 5.12: Elektriciteitsnet Simulator Hardware [eigen bron].

Door de feitelijke combinatie van een Digital Twin van een elektriciteitsnet, hard-ware-in-the-loop en de verschillende software componenten binnen een stuk IT-netwerk is de positie van de Control Room of the Future wereldwijd uniek. Zo kan de Cyber Range gebruikt worden voor verschillende gebruiksdoeleinden, zo wordt het ingezet om de cascade effecten van cyberaanvallen op het elektriciteitsnet beter te begrijpen, het testen van nieuwe energiebeheersytemen, en het ontwikkelen van nieuwe operationele technologieën, het ontwikkelen en testen van cyber aanvalsdetectie methoden, en het opleiden en trainen van personeel. Op basis van de veelzijdige toepassingsmogelijkheden en de aanpasbaarheid aan verschillende gesimuleerde (cyber) scenario's, hebben we geconcludeerd dat de control room of the future, zoals gedefinieerd door ECSO in hoofdstuk 9, kan worden beschouwd als een Cyber Range.

5.3.3 Cyber Ranges die in meerdere sectoren toegepast worden

Cyber Integration, Test and Evaluation Framework
RHEA heeft de Cyber Integration, Test and Evaluation Framework (CITEF) ontwikkeld, een Cyber Range die organisaties in staat stelt hun cybersecurity-skill te verbeteren en hen in staat stelt om tests uit te voeren op het gebied van cyberbeveiligingsincidenten en -respons [43]. Bovendien kan de omgeving worden gebruikt voor het uitvoeren van penetratietesten in een veilige omgeving. De Cyber Range wordt geleverd met een bibliotheek van virtuele assets, waardoor gebruikers of organisaties via de gebruikersinterface (zie figuur 5.13) hun eigen netwerken kunnen opzetten en scenario's kunnen ontwikkelen om bijvoorbeeld te testen kunnen op een representatieve IT-architectuur van een organisatie.



Figuur 5.13: Rhea CITEF Cyber Range user interface. Uit [78].

Airbus Cyber Range
Het Airbus Cyber Range[7] [44] platform is een multi-role cyber-simulatieplatform dat is ontwikkeld om IT/OT-systemen te modelleren bestaande uit tientallen tot honderden virtuele componenten. De Cyber Range kan gebruikt worden om realistische scenario's af te spelen, inclusief realistische cyberaanvallen. Als systeemintegrator heeft Airbus CyberSecurity de CyberRange ontwikkeld als een duurzaam industrieel product met als belangrijkste doelstellingen: configureerbaarheid (voor zowel IT als OT), en eenvoudige bediening.

AIT Cyber Range
Austrian Institute of Technology (AIT) heeft een digitaal en hybride Cyber Range[8] ontworpen die kan worden ingezet voor cyber oefeningen [45, 46, 47]. De faciliteit heeft plaats voor maximaal vierentwintig deelnemers, waarbij de deelnemers toegang hebben tot de AIT Cyber Range. Op de Cyber Range kunnen verschillende praktische oefeningen worden uitgevoerd. De AIT Cyber Range ondersteunt verschillende dynamische scenario's en oefeningen. De oefeningen kunnen op verschillende manieren worden opgezet omdat de AIT Cyber Range via hun virtuele omgeving configureerbaar is, waarbij ze voornamelijk gericht zijn op het gebruik van open source software technologie. Naast oefeningen kan de Cyber Range worden toegepast voor trainings- en educatiedoeleinden door bijvoorbeeld de Cyber Range in te richten als een reflectie van IT of OT-productieomgeving.

De trainingsinhoud kan vervolgens dan theoretisch als praktisch zijn met voorbeelden, waarbij de AIT Cyber Range al is ingezet in cybersecurity-lessen over incident response, netwerk beveiliging, en malware analyse. Verder kunnen via de AIT Cyber Range ook trainingen worden gedaan voor industrie specifieke omgevingen, om zo de kennis op cybervlak van werknemers te vergroten. Een derde doeleind waar de Cyber Range voor wordt gebruikt volgens volgens Leitner et al. [45, 47]is voor simulatie en detectie van cyberaanvallen in ICS-omgevingen. Hiervoor kan de Cyber Range worden geïntegreerd met

[7] Video van Airbus Cyber Range demonstratie: https://youtu.be/37yPDcoD6Q8
[8] Video van AIT Cyber Range demonstratie: https://youtu.be/goc50dmAYpI

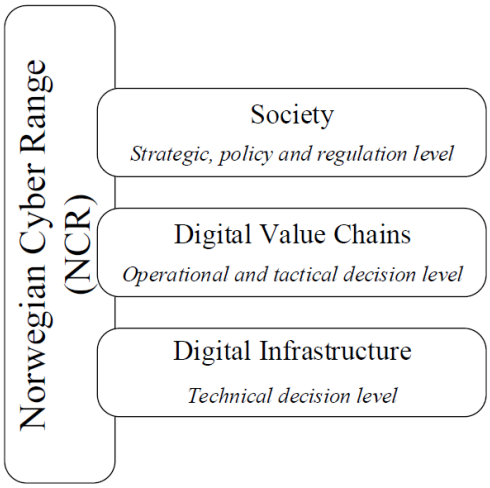
extra fysieke industriële hardware componenten in een zogenoemde ´hardware in the loop' configuratie. De integratie van zowel software als hardware faciliteert de gebruikers om gerichte aanvallen te lanceren op een representatieve ICS-omgeving en hiermee inzicht te verkrijgen in de potentiële consequenties voor de OT-omgevingen die zich binnen de installatie bevinden, hierdoor kan het gemakkelijk worden gemaakt om veiligheidscontroles te evalueren. Leitner et al. [45, 47] stellen dat de mogelijkheid om verschillende cyberomgevingen met variaties te genereren op de Cyber Range, bijdraagt aan de evaluatie van aanvalsdetectie. De beschikbaarheid diverse omgevingen, maakt het mogelijk om afzonderlijke datasets te genereren voor training, validatie en testen, waardoor de robuustheid van de evaluatieresultaten kan worden verbeterd.

5.3.4 Academische, Onderzoek en Open-Source Cyber Ranges

Norwegian Cyber Range

Het Norwegian Cyber Range (NCR) is een interdisciplinaire (cyber) arena die tot doel heeft de kwaliteit van onderwijs, training, oefeningen, testen en onderzoek op het gebied van cyberbeveiliging te verbeteren door het bieden van meer realistische omgevingen [48]. Het Norwegian Cyber Range (NCR)[9] onderscheidt zich van een normale, pure technische Cyber Range door een meer socio-technische benadering waarbij oorzaak, gevolg en dynamische relaties tussen componenten, mensen en organisaties gesimuleerd kunnen worden. Het gebruik van een socio-technische benadering heeft volgens Kianpour et al. [48] belangrijke voordelen bij het onderzoeken van de factoren die ten grondslag liggen aan de vele aspecten van cyberbeveiliging. De Cyber Range is opgedeeld in drie verschillende niveaus, zie figuur 5.14, waarbij "society level" een weerspiegeling is van maatschappelijke structuren, hier kan de impact worden gesimuleerd van cyberincidenten, de mogelijke kettingreacties en gevolgen op verschillende niveaus van de samenleving. Om de werkelijkheid accuraat te kunnen weergeven en de gevolgen van beveiligingsincidenten en bedrijfsacties te begrijpen, is kennis van de samenstelling van de reële waardeketen en de mate waarin de betrokken actoren met elkaar verbonden zijn van groot belang. "Digital Value Chains Level" modelleert uitgebreide netwerken van producenten en consumenten van digitale diensten, die zich vaak uitstrekken over sectoren, bedrijfstakken en bedrijven heen. Ten slotte is er de "digital infrastructure layer" die IT-infrastructuur van organisaties kan simuleren.

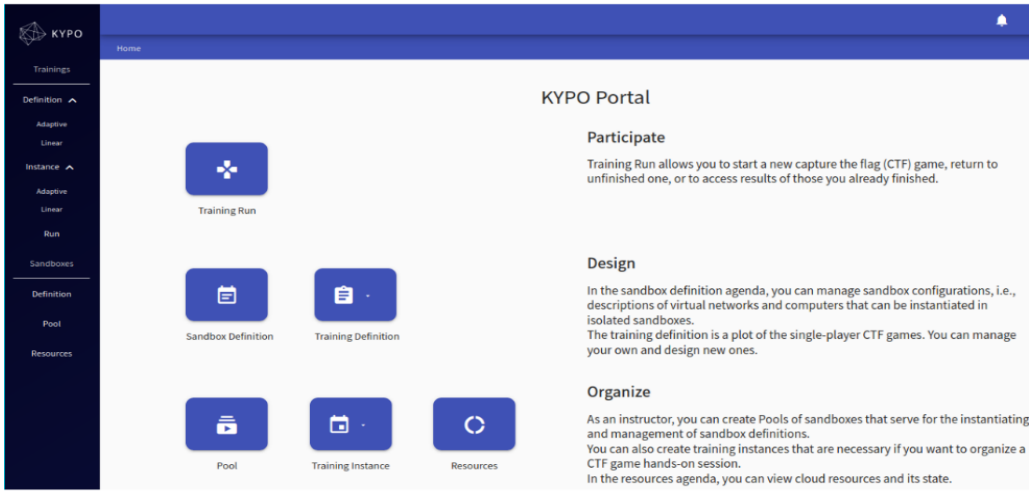
[9] Video van NCR Cyber Range demonstratie https://youtu.be/nJGgc3h0TBQ



Figuur 5.14: Noorse Cyber Range. Uit [48].

KYPO Cyber Range Platform

Het KYPO Cyber Range platform[10] (zie figuur 5.16) voor het eerst geïntroduceerd door Masaryk University is een Cyber Range waarvan de broncode[11] volledig open is, oftewel Open-Source is [49]. Vykopal et al. [50] publiceerde in hun paper: *Scalable Learning Environments for Teaching Cybersecurity Hands-on* een derde iteratie van de Cyber Range dat kan worden gebruikt voor cybersecurity-lessen, blue team trainingen of kan worden ingezet als interactieve leeromgeving met tutorials en spellen met als hoofddoel educatie. Figuur 5.15 laat een screenshot zien van de interface.



Figuur 5.15: Cyber Range User Interface. Uit: Screen capture uit video demonstratie in footnote 6.

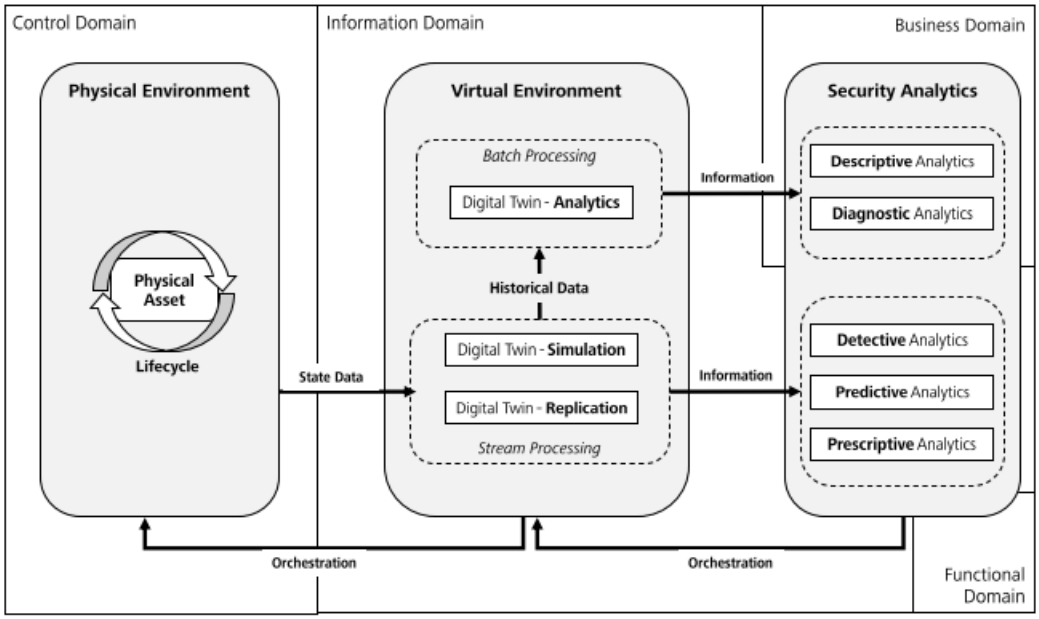
[10] Video demonstratie KYPO Cyber Range Platform: https://youtu.be/II5HTjHVPd8
[11] Broncode KYPO Cyber Range: https://gitlab.ics.muni.cz/muni-kypo-crp

Figuur 5.16: KYPO Cyber Range met hardware in the loop. Uit [49].

De Vykopal et al. [50] stellen dat het platform schaalbaar is en zowel lokaal als in de cloud kan worden ingezet. Hierdoor kunnen veel studenten leren in een kleine CR omgeving of minder studenten in een uitgebreide of complexe CR omgeving, afhankelijk van de behoefte van de eindgebruiker. Het platform maakt het mogelijk voor studenten om te oefenen vanaf hun school, werkplek, huis of andere locaties die verbonden zijn met het internet. Bovendien kan de omgeving herhaaldelijk worden gecreëerd voor verschillende klassen op grote schaal of on-demand voor elke individuele leerling.

5.4 Digital Twins in de context van cybersecurity

Digital Twins kunnen ook in verschillende vormen worden ingezet voor analyse en controle van (cyber) security toepassingen. In [51] worden Digital Twins als een recente trend in cybersecurity gezien. Aan de ene kant leidt het gebruik van Digital Twins tot nieuwe risico op het gebied van (cyber)veiligheid, terwijl ze aan de andere kant ook een middel kunnen zijn tot het analyseren, simuleren en repliceren van use cases als intrusie detectie, testen en trainen.



Figuur 5.17: DT2SA architectuur model. Uit [51].

Ook in [52] worden verschillende risico's en toepassingen van Digital Twins met betrekking tot cybersecurity genoemd. Risico's hebben met name te maken met inbreuk op confidentialiteit en eigendom van data, de veiligheid van de communicatie tussen digitale en fysieke twin, en de mogelijkheid dat kwaadwilligen via de Digital Twin zwakheden in het fysieke systeem kunnen identificeren. Omdat de Digital Twin een replica is van de fysieke twin, is het identificeren van mogelijk zwakke plekken in het systeem tegelijkertijd ook een positieve toepassing wanneer het gebruikt wordt door de eigenaar van de Digital Twin. Op deze manier kan de Digital Twin bijvoorbeeld bijdragen aan een beter 'patch management'. Digital Twins kunnen bovendien worden ingezet om een nieuw component uitvoerig te testen in het kader van risico management en incident respons management. Een andere toepassing is dat in gebruikname van fysieke systemen efficiënter kan worden gedaan door middel van Digital Twins omdat de veiligheidsaspecten kunnen worden getest.
Digital Twins kunnen ook worden gebruikt in combinatie met AI (kunstmatige intelligentie) en ML (machine learning) om real-time detectie van bijvoorbeeld cyberaanvallen of andere verdachte veranderingen in het fysieke systeem te herkennen. Deze toepassingen van Digital Twins zijn nog relatief nieuw, maar bieden veel kansen voor operationele omgevingen [53].

Voorbeelden van geïmplementeerde Digital Twins in het domein van cybersecurity zijn nog relatief schaars [54]. Wel zijn er naast de genoemde conceptuele artikelen, voorbeelden waarin meer concreet architecturen worden ontwikkeld. In [55] wordt een benadering voor het repliceren van een cyber-physical systeem en hoe aanvallen op het systeem kunnen worden gedetecteerd. Ook in [56] wordt een proof-of-concept systeem ontwikkeld dat een helpt om nieuwe technische regels te ontwikkelen voor het fysieke systeem op basis van simulaties van aanvallen. Verschillende voorbeelden van stress-testing platforms gebaseerd op Digital Twin technologie worden genoemd in [57], waaronder EPANET en RISKNOUGHT, die bedoeld zijn om verschillende gevaren die afkomen op SCADA-systemen in de watersector te testen.

Verdere uitwerking van kansen voor de gecombineerde inzet van Cyber Ranges en Digital Twins wordt in hoofdstuk 6 beschreven.

5.5 Reflectie

Deze paragraaf reflecteert op de aspecten, overeenkomsten en verschillen.

De afbakening tussen de twee technologieën blijkt in alle aangehaalde bronnen niet altijd even duidelijk. Uit dit onderzoek zijn drie redenen af te leiden die tot deze begripsverwarring bijdragen:

1. Zowel Digital Twins als Cyber Ranges werken met een model van de werkelijkheid.
2. De term Digital Twin heeft zich in de afgelopen jaren tot een 'hot topic' ontwikkeld. Er zijn in de academische wereld veel artikelen over Digital Twins die het potentieel van deze technologie schetsen. Er is echter wel een groot verschil zichtbaar in commerciële en populaire media-uiting rondom Digital Twins en de ontwikkeling en discussie hierover in de academische wereld. Dit geeft aan dat dit veld sterk in ontwikkeling is en hier de komende jaren veel technologische ontwikkeling is te verwachten.
3. De standaardisatie van het Digital Twin concept is nog in volle gang bij formele standaardisatie organen. Op nationaal gebied is de NEN [58] actief en ISO [59] op internationaal niveau. Hierdoor bestaat nog geen algemeen geaccepteerde definitie die kan helpen bij de afbakening van de twee technologieën.

Hoe kan ondanks de begripsverwarring een logisch verschil tussen de twee technologieën gemaakt worden? Het belangrijkste verschil tussen Digital Twins en Cyber Ranges ligt in het gebruik: hun respectievelijke doeleinden en toepassingen. Een Cyber Range is hoofdzakelijk ontworpen voor cybersecurity-training en -simulatie. Het biedt een gecontroleerde omgeving om cyberaanvallen te simuleren, verdedigingsmechanismen te testen en professionals op te leiden in het reageren op en beperken van beveiligingsbedreigingen. Daarnaast wordt een Cyber Range ingezet bij het testen van (nieuwe) netwerkapparatuur en (nieuwe) processen.

Digital Twins daarentegen richten zich niet specifiek op het cybersecurity-domein. Een Digital Twin wordt gebruikt voor de optimalisatie van primaire operationele bedrijfsprocessen door een virtuele representatie te maken van een fysiek object, proces of systeem om de prestaties van de echte entiteit die het vertegenwoordigt te monitoren, analyseren en optimaliseren.

In de watersector zijn wereldwijd tot nu toe alleen enkele voorbeelden van Cyber Ranges bekend. In eerste instantie werden deze simulatieomgevingen als Testbed voor onderzoeksdoeleinden opgezet, maar worden inmiddels ook als Cyber Range voor oefeningen en trainingen geconfigureerd. De Nederlandse watersector maakt momenteel nog geen gebruik van een Cyber Range die specifiek ontworpen is voor de watersector.

Digital Twins worden daarentegen zowel in het binnen- als buitenland in de watersector toegepast voor de optimalisatie van primaire bedrijfsprocessen, zoals in paragraaf 5.2 is beschreven. Het meest prominente binnenlandse voorbeeld is het inzetten van Digital Twins door drinkwaterbedrijf Vitens. Vitens zet Digital Twins in voor controle van waterproductie, -kwaliteit, -distributie en de controle van de staat pijpleidingen. In de academische wereld zijn wij één voorbeeld tegengekomen waarin een open-source Digital Twin van een drinkwater distributie system gebruikt kan worden voor cybersecurity-doeleinden (zie hoofdstuk 5.2.3). Er zijn echter wereldwijd geen Digital Twins bekend die voor cybersecurity-doeleinden in de watersector ingezet worden.

6 Kansen of ontwikkelrichtingen voor de Watersector

In dit rapport zijn de concepten van Cyber Ranges en Digital Twins als twee losstaande begrippen uitgewerkt. De auteurs van dit rapport zien voor de watersector potentie in zowel de toepassing van de twee technologieën op zichzelf, als ook het combineren van beide technieken.

Door de toename van cyberaanvallen in de afgelopen jaren, is ook de urgentie toegenomen om functionaliteit in systemen toe te voegen, of software te patchen. Daarnaast is voor veel bedrijven en organisaties, evenals voor de watersector, het landschap van de te verdedigende digitale infrastructuur groter en complexer geworden. De infrastructuur omvat niet alleen IT/kantoor- en OT-omgevingen, maar ook bijvoorbeeld cloud- en mobiele infrastructuur. Daarbij worden van OT-softwaresystemen hoge eisen van beschikbaarheid verwacht. Deze uitdagingen en vereisten vragen om werkwijzen waarmee veranderingen die een impact hebben op het operationele proces snel getoetst kunnen worden.

Deze verkenning naar Cyber Ranges en Digital Twins heeft een zestal kansen geïdentificeerd voor de watersector. De kansen zijn in het kader van deze theoretische verkenning nog niet getoetst met de watersector en vormen daarom vooral ontwikkelrichtingen die de watersector verder kan exploreren. De kansen zijn in onderstaande tabel onderverdeeld in korte, middellange en lange termijn uitvoerbaarheid, afhankelijk van de complexiteit van hun implementatie. Dit is ook de reden waarom Digital Twins pas vanaf kans 5 hun intrede doen.

Tabel 6.1: Overzicht kansen of ontwikkelrichtingen.

Korte termijn
❯ Kans 1: Watersector-specifieke Cyber Range voor training van personeel. ❯ Kans 2: Cyber Range voor het oefenen en verbeteren van incident-response procedures. ❯ Kans 3: Cyber Range in een OTAP-omgeving om cyberrobuustheid en -gedrag van nieuwe componenten te testen.
Middellange termijn
❯ Kans 4: Cyber Range voor het experimenteren met gepubliceerde kwetsbaarheden. ❯ Kans 5: Simulatie van effecten van cyberaanval op primaire bedrijfsprocessen.
Langere termijn
❯ Kans 6: Digital Twins voor het detecteren van anomalieën en cyberaanvallen in real-time.

Korte termijn - kans 1: Watersector-specifieke Cyber Range voor training van personeel
Een Cyber Range is specifiek ontworpen om IT- en cybersecurity-personeel te trainen om vaardigheden te ontwikkelen en te verbeteren voor het ontdekken en verdedigen tegen cyberaanvallen. Theoretisch gezien kan personeel in de Nederlandse watersector oefenen op een generieke Cyber Range die door een andere organisatie gerund wordt. De meerwaarde ligt in het opzetten van een specifieke Nederlandse Watersector Cyber Range, omdat deze dan herkenbare en realistische componenten en tools uit de infrastructuur van de watersector gebruikt. Hierbij zou onderscheid gemaakt kunnen worden voor een Cyber Range voor de drinkwaterbedrijven en een Cyber Range voor de subsector "Keren en beheren", waaronder Rijkswaterstaat en de waterschappen vallen.

Als randvoorwaarden voor het gebruik van een Cyber Range geldt altijd dat:
- De doelstelling(en) duidelijk moet(en) zijn voor het gebruik van de Cyber Range (bijvoorbeeld, of de Cyber Range alleen voor trainingsdoeleinden gebruikt zal kunnen worden, of ook voor andere doeleinden zoals in hoofdstuk 3.1 beschreven. Maar ook welke specifieke vaardigheden en welke gebruikersgroepen getraind worden.)
- Voldoende middelen beschikbaar gemaakt moeten worden om de Cyber Range op te bouwen, te bedienen en te onderhouden, zoals budget voor de Cyber Range componenten en personeel met de juiste expertise. Bij een watersector-specifieke Cyber Range moet ervoor gezorgd worden dat de juiste componenten en tools gebruikt worden.
- De Cyber Range up-to-date moet zijn om realistische scenario's te kunnen oefenen. Dat betekend dat er een proces moet zijn die ervoor zorgt dat bijvoorbeeld de impact van de nieuwste cybersecurity-bedreigingen en trends op de samenstelling van de Cyber Range en oefenscenario's beoordeeld worden. Daarnaast moet de Cyber Range infrastructuur net zoals een echte netwerkomgeving regelmatig geüpdatet worden.

Vanuit de Network and Information Security Directive 2 (NIS2) zijn basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging een onderdeel in vereiste risicobeheersmaatregelen [60]. Met een centrale Cyber Range kan de Watersector zijn personeel over verschillende organisaties heen op een vergelijkbare manier trainen en zo aan de (toekomstige) Nederlandse vertaling van de NIS2 eisen voldoen, terwijl de kosten voor het opzetten en beheer van de Cyber Range gezamenlijk gedragen kunnen worden.

Korte termijn – kans 2: Cyber Ranges voor het oefenen en verbeteren van incident-response procedures
Naast het trainen van personeel kan een Cyber Range ook gebruikt worden om incident-response procedures te testen en te verbeteren binnen de eigen organisatie. Dit kan verder uitgebreid worden om ook samen met ketenpartners en toeleveranciers te oefenen. Daarvoor zal een Cyber Range-oefenscenario gecombineerd worden met een table-top oefening. Op deze manier wordt cybersecurity-personeel uit de eigen organisatie en ketenpartners/toeleveranciers in staat gesteld zich op een cyberincident voor te bereiden en daardoor communicatie, handelingen en hun verantwoordelijkheden te oefenen.
Hiervoor gelden dezelfde randvoorwaarden als kans 1. Daarnaast:
- moeten incident-response procedures (zoals response-playbooks) bestaan die getest kunnen worden;
- moeten afspraken met ketenpartners/toeleveranciers gemaakt worden voor het oefenen.

Procedures t.b.v. incidentbehandeling zijn onderdeel van de vereiste risicobeheersmaatregelen in de NIS2 [60]. Een Cyber Range biedt de mogelijkheid om praktische ervaring op te doen met theoretisch opgezette incident-response procedures.

Korte termijn - kans 3: Cyber Range in een OTAP-omgeving om cyberrobuustheid en -gedrag van nieuwe componenten te testen
Bij de ontwikkeling van operationele software systemen wordt gebruik gemaakt van technieken om grotendeels geautomatiseerd veranderingen door te kunnen voeren zonder de bedrijfsvoering in gevaar te brengen. Door vooraf te kunnen testen welke effecten veranderingen, zoals bijvoorbeeld beveiligingspatches, teweegbrengen, kan een betere bepaling worden gemaakt van de impact op bijvoorbeeld operationele systemen. Dit proces kan ook worden doorlopen wanneer er bijvoorbeeld nieuwe OT- of IT-componenten getest moeten worden. De eventuele effecten die nieuwe componenten met zich meebrengen kunnen op deze manier vooraf beter worden begrepen.

Om dit geautomatiseerd te kunnen doen wordt onderscheid gemaakt in *Ontwikkel-, Test-, Acceptatie- en Productie-omgevingen,* afgekort met OTAP (of in het Engels DTAP: Development, Testing, Acceptance and Production). Daarbij worden ook vaak de begrippen *Continuous Integration (CI)* en *Continuous Delivery (CD)* gebruikt, waarbij er geen harde scheiding meer is tussen de ontwikkel systemen en operationele systemen.

Figuur 6.1: Typische cyclus van Continuous Integration (CI) en Continous Delivery (CD) wanneer een OTAP-straat volledig geautomatiseerd is.

OTAP-omgevingen zijn bedoeld om nieuw ontwikkelde softwarefunctionaliteit op hun correctie functionaliteit te testen, in een omgeving die afgeschermd is van de productieomgeving [61] [62].

En Cyber Range kan een onderdeel uitmaken van de test en acceptatie fase in het OTAP-proces, waar een nieuwe software of hardwarecomponent doelgericht op haar cyberrobuustheid en cyberrelevante gedrag getest wordt. Het gaat hier dus niet om het testen op fouten en beoogde doelstelling van de nieuwe component, maar om het inzichtelijk krijgen hoe een nieuwe component bij een cyberaanval reageert, of welk gedrag een nieuw component naast de beoogde functionaliteit toont dat de cyberweerbaarheid van het hele systeem kan beïnvloeden. Een voorbeeld is een nieuw systeemcomponent welke regelmatig een communicatiekanaal opent om diagnostische data aan zijn fabrikant terug te koppelen. Het kan een bewuste keuze zijn om communicatie tussen het component en de fabrikant toe te laten, maar het testen in een Cyber Range maakt deze functionaliteit en bijhorende risico's inzichtelijk en bespreekbaar.

En Cyber Range vervangt dan ook niet het OTAP-proces, waarin nieuwe functionaliteit eerst afgeschermd op functionaliteit getest wordt voordat het in de operationele productieomgeving geïmplementeerd wordt. De doelstellingen van een Cyber Range dienen veel meer als toevoeging aan het OTAP-proces. Het is echter wel denkbaar om een netwerksimulatieomgeving zo in te richten dat het zowel aan de doelstelling van een OTAP-proces, als ook aan de doelstelling van een Cyber Range voldoet.

Hiervoor gelden dezelfde randvoorwaarden als kans 1. Daarnaast:
- moet er meer tijd gereserveerd worden waarmee cybersecurity-personeel vertrouwd kan raken met nieuwe componenten.

Een Cyber Range zou dus heel goed onderdeel uit kunnen maken van een OTAP-proces, en zo helpen om aan de risicobeheersmaatregelen in de NIS2 te voldoen die vereist dat er beveiliging bestaat bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen.

Middellange termijn - kans 4: Cyber Range voor het experimenteren met gepubliceerde kwetsbaarheden
Een Cyber Range biedt de mogelijkheid om met gepubliceerde kwetsbaarheden te experimenteren om de problematiek beter te begrijpen en vervolgens mitigerende maatregelen te bedenken.

In de toekomst zou het misschien zelfs mogelijk zijn om in een Cyber Range die de IT- en/of OT-omgeving van een drinkwaterbedrijf of waterschap nauwkeurig simuleert, specifieke aanvalsscenario's op gepubliceerde kwetsbaarheden te testen, de effectiviteit van beveiligingsmaatregelen te onderzoeken, en de impact van een kwetsbaarheid op de organisatie te beoordelen.

Hiervoor gelden dezelfde randvoorwaarden als kans 1. Daarnaast:
- moet de Cyber Range een zo nauwkeurig mogelijke representatie kunnen gebruiken van de IT- en/of OT-omgeving (of een afgebakend onderdeel daarvan). Enkel dan kan effectief onderzoek gedaan worden naar de effecten van beveiligingsmaatregelen en de mogelijke impact ervan op een organisatie. Om dit mogelijk te maken moet het asset- en configuratiemanagement op orde zijn, zodat bekend is uit welke software- en hardwarecomponenten de IT- en/of OT-omgeving bestaat. De toenemende complexiteit van software systemen en gebrek aan een systematische aanpak om inzicht in de samenstelling van al deze systemen te verkrijgen heeft echter als gevolg dat het asset- en configuratiemanagement voor veel organisaties een uitdaging blijft. Hierbij kan op termijn de verplichting uit de Cyber Resilience Act behulpzaam zijn, waarin een vereiste voor softwareleveranciers is opgenomen om een Software Bill of Material (SBOM) te leveren [63]: in een SBOM staat beschreven welke software componenten gebruikt zijn in een software product.

Deze meer geavanceerdere manier van gebruik van een Cyber Range kan bijdragen aan de NIS2 vereisten rondom het hebben van beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen [60].

Middellange termijn - kans 5: Simulatie van effecten van cyberaanval op primaire bedrijfsprocessen
Zoals uit de definitie van een Digital Twin blijkt (zie hoofdstuk 2), bevat een Digital Twin een virtuele representatie van (een deel van) een fysiek systeem. Een Digital Twin kan daarmee dus een representatie van een component in het primaire productieproces zijn.
Indien de watersector in toenemend mate gebruik maakt van Digital Twins om operationele processen te optimaliseren, dan zou het voordelig zijn om deze investering ook te gebruiken in een Cyber Range omgeving, om effecten van potentiële cyberaanvallen op primaire bedrijfsprocessen (bijvoorbeeld de waterkwaliteit) te kunnen achterhalen.
Daarnaast biedt de integratie van een Digital Twin in een Cyber Range omgeving ook de kans om multidisciplinair te oefenen met medewerkers uit het primaire proces, IT-personeel en het crisismanagement team.

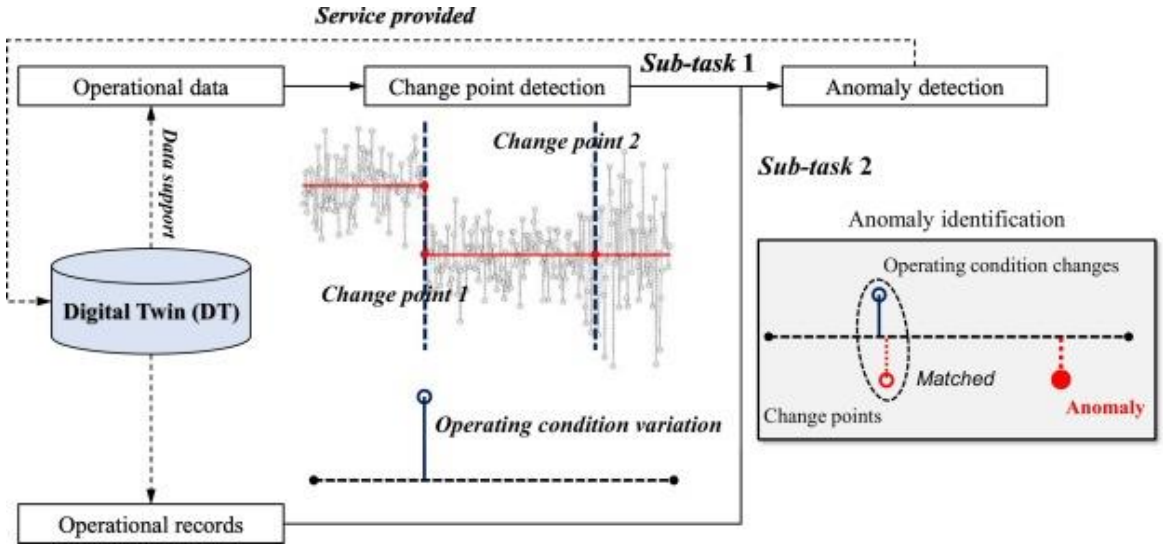
Wat betreft de Cyber Range gelden dezelfde randvoorwaarden als kans 1. Daarnaast:
- zijn de uitdagingen die in hoofdstuk 5.2 voor de succesvolle inzet van het Digital Twin genoemd zijn (datakwaliteit, verbinding tussen fysieke entiteit en Digital Twin, up-to-date houden van Digital Twin simulatiemodel) randvoorwaardelijk voor een realistische simulatie.

NIS2 vereist risicobeheersmaatregelen ten behoeve van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer. Door met multidisciplinaire teams te oefenen kunnen noodvoorzieningsplannen en crisisbeheersmaatregelen getraind en aangescherpt worden zodat aan de NIS2 eis wordt voldaan en de bedrijfscontinuïteit gewaarborgd is. Simulatie van effecten die nauw aansluiten bij fysieke processen uit de bedrijfsvoering kan daar behulpzaam in zijn.

Lange termijn – kans 6: Digital Twins voor het detecteren van anomalieën en cyberaanvallen in real-time
Indien er een Digital Twin van (delen van) de operationele omgeving beschikbaar is voor procesoptimalisatie, dan is een uitbreiding voorstelbaar om deze ook in te zetten voor detectie van afwijkend gedrag (anomaliedetectie). Anomaliedetectie kan veroorzaakt worden door systeemfouten of cyberaanvallen. Een mogelijke methode om dit te bereiken, is door de Digital Twin te gebruiken als een virtueel referentiepunt waaraan het werkelijke (fysieke) systeem getoetst kan worden. Indien het verschil tussen de gemeten waardes van het (fysieke) systeem en waardes afkomstig uit de Digital Twin te veel afwijken, kan dit duiden op onjuist systeemgedrag, wat mogelijk ook veroorzaakt kan worden door een cyberaanval op de operationele omgeving.

Deze kans richt zich met name op de OT-omgeving in de lagen 0-3 van het Purdue model en heeft de volgende randvoorwaarden:
- Parameters die voor anomalie detectie getoetst moeten worden dienen beschikbaar te zijn in de Digital Twin. Dit houdt in dat relevante variabelen en metingen die nodig zijn voor het toetsen van afwijkingen ook in de Digital Twin aanwezig moeten zijn.
- De Digital Twin moet van voldoende kwaliteit zijn om betrouwbaar de (fysieke) entiteit te beschrijven, hiervoor moet de Digital Twin nauwkeurig en gedetailleerd zijn. Een onvolledige Digital Twin kan leiden tot het onjuist detecteren en classificeren van anomalieën.
- Data waarop getoetst moet worden voor anomalieën in de OT-omgeving moet beschikbaar zijn. Dit betekent dat de vereiste gegevens, zoals sensormetingen, communicatie data verzamelt wordt en beschikbaar is.

Een voorbeeld van een dergelijke toepassing waarbij een Digital Twin is gekoppeld aan een operationeel proces, ten behoeve van anomalie detectie is o.a. beschreven in [64]: *“Digital Twin-enabled anomaly detection for built asset monitoring in operation and maintenance”* en schematisch weergegeven in figuur 6.2.



Figuur 6.2: Anomaliedetectie in een operationeel proces m.b.v. Digital Twin. Uit [64].

7 Conclusies

De Nederlandse Watersector kan aan de hand van de onderzoeksbevindingen duiden wat Cyber Ranges en Digital Twins kunnen betekenen voor hun eigen bedrijfsvoering en de sector in zijn geheel. De bevindingen worden per onderzoeksvraag weergegeven.

Onderzoeksvraag 1. Wat zijn Cyber Ranges en Digital Twins en wat is het probleem dat met Digital Twins en Cyber Ranges opgelost kan worden (toepassingsmogelijkheden)?

Tijdens het onderzoek is gebleken dat beide technologieën, op vele verschillende manieren gedefinieerd en geïnterpreteerd worden, zowel in populaire media, als door fabrikanten en wetenschappelijke artikelen.

De volledigste definitie van Cyber Ranges troffen we aan bij de European Cyber Security Organisation: Een Cyber Range is een platform voor het ontwikkelen en gebruiken van interactieve simulatieomgevingen. De technologie wordt toegepast voor cybersecurity-testing, cybersecurity-onderzoek, cybersecurity-opleiding & training, ontwikkeling en beoordeling van cyberweerbaarheid, recruitment van (cyber)talent, nationale en Internationale cybersecurity-competities. Het levert een gecontroleerde omgeving waarin o.a. cyberaanvallen gesimuleerd worden, verdedigingsmechanismen getest kunnen worden en waar professionals opgeleid worden in het reageren op en beperken van beveiligingsbedreigingen.

De Wageningen University & Research definieerde Digital Twin het meest volledig: een combinatie en interactie van een fysiek systeem en een virtuele representatie van dit systeem, vaak een computermodel. Toepassingen van Digital Twins zijn niet specifiek ontwikkeld voor het cybersecurity-domein; deze worden gebruikt voor de optimalisatie van primaire operationele bedrijfsprocessen door een virtuele representatie te maken van een fysiek object, proces of systeem om de prestaties van de echte entiteit die het vertegenwoordigt te monitoren, analyseren en optimaliseren.

Het belangrijkste verschil tussen Digital Twins en Cyber Ranges ligt in het gebruik: hun respectievelijke doeleinden en toepassingen. Een Cyber Range wordt gebruikt voor cybersecurity-trainingen en -simulatie. Met een Cyber Range kunnen bedrijven uit de watersector alleen of samen activiteiten ontplooien zonder daarvoor het primaire proces te moeten gebruiken. Het kan een middel zijn om op representatieve, doch veilige manier onderzoek te doen naar bijvoorbeeld: bestaande en nieuwe kwetsbaarheden, nieuwe tooling of cybersecurity-maatregelen te testen en ontwikkelen, en om competenties op het gebied van cybersecurity-monitoring, detectie en onderhoud te onderhouden. Digital Twins worden tot op heden veelal gebruikt om de operationele bedrijfsprocessen digitaal te reproduceren teneinde monitoring, analyse en optimalisatie van processen. Om de fysieke processen zo juist mogelijk digitaal te reproduceren wordt in de literatuur gehint op het doorontwikkelen van Digital Twins. Bijvoorbeeld door data uit de fysieke wereld te integreren met operationele processen. Digital Twins die voor cybersecurity-doeleinden in de watersector ingezet worden zijn niet gevonden tijdens dit onderzoek (behalve de DHALSIM Digital Twin, deze wordt voor onderzoeksdoeleinden gebruikt). Digital Twins met een cybersecurity-focus worden met name in wetenschappelijke context onderzocht.

Onderzoeksvraag 2. Wordt er zowel in theorie als praktijk onderscheid gemaakt tussen de technologische vereisten van Digital Twin en Cyber Range technologieën afhankelijk van de gekozen toepassing?

Zowel in theorie als in praktijkvoorbeelden zien wij dat beide technologieën met een model van de werkelijkheid werken, maar dat ze zich onderscheiden in gebruik en toepassing. Om als Cyber Range toegepast te kunnen worden moet een model een aantal technologische elementen en functionaliteiten bevatten, zoals de mogelijkheid voor het creëren, genereren, bewerken, inzetten en uitvoeren van cybersecurity-scenario's, het loggen, monitoren, en verzamelen van informatie over de Cyber Range omgeving, en het aanbieden van leer- en tutorialmateriaal voor trainingsdoeleinden (zie voor een volledige lijst van technologische hoofdelementen in hoofdstuk 3.2).

Om als Digital Twin gebruikt te kunnen worden heeft een model als kenmerk dat het een kopie van een bestaande fysieke entiteit is, die zo goed mogelijk gemodelleerd wordt. De Digital Twin werkt met echte data (real-time, of uit het geschiedenis) en er zijn (real-time) connecties tussen de fysieke entiteit en de Digital Twin om synchronisatie mogelijk te maken (zie voor een volledige lijst van technologische hoofdelementen hoofdstuk 4.3). Bij aanwezigheid van deze technologische vereisten wordt een model bruikbaar als Digital Twin.

Onderzoeksvraag 3. Zijn er wereldwijd best practices of voorbeelden van onderzoeks- en of innovatieprojecten op het gebied van Cyber Ranges en Digital Twins in de watersector en andere sectoren, en wat kan de Nederlandse watersector hiervan leren?

Cyber Ranges en Digital Twins worden in uiteenlopende sectoren uitgeprobeerd en toegepast. In de watersector zijn wereldwijd tot nu toe alleen enkele voorbeelden van Cyber Ranges bekend, zoals in hoofdstuk 5.1 wordt beschreven. In eerste instantie werden deze simulatieomgevingen als testbed voor onderzoeksdoeleinden opgezet, maar worden inmiddels ook als Cyber Range voor oefeningen en trainingen geconfigureerd. De Nederlandse watersector maakt op moment van schrijven nog geen gebruik van een Cyber Range die specifiek ontworpen is voor de watersector. Een watersector-specifieke Cyber Range zoals beschreven als kans 1 in hoofdstuk 6 zou een waardevol platform bieden om cyberaanvalsscenario's relevant voor de watersector te oefenen. Dat zou een verglijkbare omgeving kunnen bieden zoals eerder beschreven testbedden in Singapore of de Verenigde staten (in hoofdstuk 5.1).

Digital Twins worden daarentegen zowel in het binnen- als buitenland in de watersector toegepast voor de optimalisatie van primaire bedrijfsprocessen, zoals in hoofdstuk 5.2 is beschreven. In de academische wereld zijn wij één voorbeeld tegengekomen waarin een open-source Digital Twin van een drinkwater distributie system gebruikt kan worden voor cybersecurity-doeleinden (zie hoofdstuk 5.2.3). Er zijn echter wereldwijd geen Digital Twins uit de praktijk bekend die voor cybersecurity-doeleinden in de watersector ingezet worden. Ter inspiratie zou daarom het in hoofdstuk 5.3.2 beschreven voorbeeld uit de energiesector kunnen dienen: het Control Room of the future van de TU Delft kan door de integratie van een Digital Twin in een Cyber Range de effecten van cyberaanvallen op het elektriciteitsnet simuleren. Deze toepassing is vergelijkbaar met kans 5 in hoofdstuk 6.

Onderzoeksvraag 4. Wat zijn de randvoorwaarden om Cyber Ranges of Digital Twins in de praktijk toe te kunnen passen?

Cyber Ranges en Digital Twins kunnen ingezet worden om organisaties cyberweerbaar te maken. Net zoals voor vele andere sectoren is het voor de Nederlandse watersector van

belang zijn primaire bedrijfsprocessen te beschermen, onder andere tegen cyberaanvallen. De watersector heeft hierbij bijzondere eisen, namelijk dat processen in de watersector een zeer hoge mate van beschikbaarheid (of uptime) moeten hebben en in staat moeten zijn om incrementele updates t.b.v. security en/of functionaliteit door te voeren.

Cyber Ranges en Digital Twins stellen organisaties in staat om met simulaties en modellen van de werkelijkheid te experimenteren om zich voor te bereiden op mogelijke cyberaanvallen, zonder dat de beschikbaarheid van primaire bedrijfsprocessen in geding komt.

In dit onderzoek zijn een zestal kansen geïdentificeerd voor de toepassing van Cyber Ranges en Digital Twins. Deze zijn onderverdeeld in korte-, middellange en lange termijn kansen. Met deze kansen zijn ook de randvoorwaarden om Cyber Ranges of Digital Twins in de praktijk toe te kunnen passen opgenomen.

Tabel 7.1: Samenvatting van de kansen en randvoorwaarden van Cyber Ranges en Digital Twins voor de watersector.

#	Naam van de kans	Doelstelling	Scope (binnen organisatie / extern)	Randvoorwaarden
Korte termijn				
1	Watersector-specifieke Cyber Range voor training van personeel	Mogelijkheden om voor de watersector realistische en uitdagende oefeningen op te zetten een voorbereiding op NIS2	Intern	• Duidelijke doelstelling voor beoogde resultaten met Cyber Range • Voldoende middelen voor het opzetten en onderhouden van Cyber Range • Proces voor het up-to-date houden van Cyber Range
2	Cyber Range voor het oefenen en verbeteren van incident-response procedures	Verhogen van de (keten)weerbaarheid en voorbereiding op NIS2	Intern & extern	Dezelfde als Kans 1 + • Beschikbaarheid van incident-response procedures • Afspraken met ketenpartners/toeleveranciers
3	Cyber Range in een OTAP-omgeving om cyberrobuustheid en -gedrag van nieuwe componenten te testen	Ondersteunen van proces om nieuwe functionaliteit/apparatuur in operationele omgeving toe te voegen en voorbereiding op NIS2	Intern & extern	Dezelfde als Kans 1 + • Extra tijd om kennis over nieuwe functionaliteit/apparatuur op te bouwen
Middellange termijn				
4	Cyber Range voor het experimenteren met gepubliceerde kwetsbaarheden	Beter begrijpen van kwetsbaarheden en mogelijke voorbereiding op NIS2	Intern	Dezelfde als Kans 1 + • Nauwkeurige kopie van IT-OT-omgeving (o.b.v. uitgebreid asset- en configuratiemanagement).
5	Integreren Digital Twins met Cyber Ranges om effecten van cyberaanval op primaire bedrijfsprocessen te simuleren	Inzichtelijk maken van effecten van cyberaanvallen op primaire bedrijfsprocessen, multidisciplinair oefen en voorbereiding op NIS2	Intern	Dezelfde als Kans 1 + • Goede data kwaliteit van de Digital Twin • Connectie tussen fysieke entiteit en Digital Twin • Up-to-date Digital Twin simulatiemodel
Lange termijn				
6	Digital Twins voor het detecteren van anomalieën en cyberaanvallen in real-time	Real-time detectie t.b.v. verbeterde monitoring en snellere response op incidenten	Intern	• Goede data kwaliteit van de Digital Twin • Connectie tussen fysieke entiteit en Digital Twin • Up-to-date Digital Twin simulatiemodel • Beschikbaarheid van parameters voor anomaliedetectie in Digital Twin en fysieke omgeving

Bij de presentatie van de resultaten van deze verkenningsstudie op 19 juni 2023 aan experts bij het Ministerie I&W en vertegenwoordigers uit de watersector werd kans 5 als meest waardevol beoordeeld. Kans 3 (dicht gevolgd van kans 2 en 5) werd gezien als kans die het beste kan ondersteunen om aan wetgeving en richtlijnen in de watersector te voldoen.

Bibliografie

[1] M. van Infrastructuur en Waterstaat, „Programma Versterken Cyberweerbaarheid in de Watersector 2019 – 2022,” p. 14, November 2020.

[2] E. C. S. O. (ECSO), „Understanding Cyber Ranges: From Hype to Reality,” *SWG 5.1 I Cyber Range Environments and Technical Exercises,* 2020.

[3] WUR, „Digital Twin voor Waterbeheer,” Wageningen Universiteit, 15 Maart 2022. [Online]. Available: https://www.wur.nl/nl/onderzoek-resultaten/onderzoeksinstituten/environmental-research/show-wenr/digital-twin-voor-waterbeheer.htm. [Geopend April 2023].

[4] N. I. o. S. a. Technology, „Cyber Ranges,” Nist, 13 02 2018. [Online]. Available: https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf. [Geopend 30 1 2023].

[5] N. I. f. C. E. (. C. R. Team, „The Cyber Range: A Guide,” NIST, 2020. [Online]. Available: https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf. [Geopend 30 1 2023].

[6] KPN, „Cybersecurity trainen op een Cyber Range: zo doet KPN dat,” KPN, [Online]. Available: https://jobs.kpn.com/nl/nl/article-cybersecurity-trainen-op-een-cyber-range-zo-doet-kpn-dat. [Geopend 21 2 2023].

[7] J. Päijänen, „CyberSec4Europe - D7.6 Collection of agreements, guidance documentation and dissemination materials,” p. 32, June 2022.

[8] M. M. Yamin, B. Katt en V. Gkioulos, „Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” *Computers & Security,* vol. 88, p. 101636, 2020.

[9] E. Ukwandu, M. A. B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic en X. Bellekens, „A Review of Cyber-Ranges and Test-Beds: Current and Future Trends,” *Sensors,* vol. 20, 2020.

[10] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri en S. Lightman, „NIST SP 800-82r3 ipd Guide to Operational Technology (OT),” *NIST Special Publication,* p. 317, April 2022.

[11] Gartner, „Gartner Glossary - Digital Twin,” 2022. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/digital-twin. [Geopend 05 06 2023].

[12] Digital Twin Consortium, „digital twin consortium,” [Online]. Available: https://www.digitaltwinconsortium.org/. [Geopend 05 06 2023].

[13] KWR, „Digitale tweeling voor de zuivering,” [Online]. Available: https://www.kwrwater.nl/projecten/digitale-tweeling-voor-de-zuivering/. [Geopend 05 06 2023].

[14] Q. Qi, F. Tao, T. Hu, N. Anwer, A. Liu, Y. Wei, L. Wang en A. Nee, „Enabling technologies and tools for digital twin,” *Journal of Manufacturing Systems,* vol. 58, nr. B, pp. 3-21, 2021.

[15] P. Pileggi, E. Lazovik, J. Broekhuijsen, M. Borth en J. Verriet, „Lifecycle Governance for Effective Digital Twins: A Joint Systems Engineering and IT Perspective," in SysCon 2020, The 14th Annual IEEE International Systems Conference, April 20 - 23, 2020, Montréal, Québec, Canada, 2020.

[16] G. Karmous-Edwards, D. Fortune, S. Ramboz en et al., „Digital Twin Readiness Guide," SWAN, West Sussex, UK, 2022.

[17] A. P. Mathur en N. O. Tippenhauer, „SWaT: a water treatment testbed for research and training on ICS security," in *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, 2016.

[18] C. M. Ahmed, V. R. Palleti en A. P. Mathur, „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*, New York, NY, USA, 2017.

[19] D. Li, D. Chen, L. Shi, B. Jin, J. Goh en S.-K. Ng, „MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks," *CoRR,* vol. abs/1901.04997, 2019.

[20] J.-P. Konijn, Multi-domain Cyber-attack Detection in Industrial Control Systems, 2022.

[21] S. Adepu, N. K. Kandasamy en A. Mathur, „EPIC: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security," in *Computer Security*, Cham, 2019.

[22] „Inaugural CIDeX 2022 held at NUS School of Computing to tackle cyber warfare," National University of Singapore, 28 11 2022. [Online]. Available: https://www.comp.nus.edu.sg/news/2022-inaugural-cidex-2022/. [Geopend 20 2 2023].

[23] M. Singapore, „National Agencies Tackle Cyber Threats at Inaugural Cyber Defence Exercise; DIS and CSA Sign Joint Operations Agreement for Cyber Cooperation," 16 11 2022. [Online]. Available: https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/November/16nov22_nr. [Geopend 20 2 2023].

[24] „CISS - Critical Infrastrcuture Security Showdown 2023," [Online]. Available: https://itrust.sutd.edu.sg/ciss-2023/. [Geopend 13 06 2023].

[25] V. Giuliano en V. Formicola, ICSrange: A Simulation-based Cyber Range Platform for Industrial Control Systems, arXiv, 2019.

[26] „Idaho National Laboratory - Water Security Testbed," 2021. [Online]. Available: https://factsheets.inl.gov/FactSheets/Water%20Security%20Test%20Bed%202021.pdf. [Geopend 05 06 2023].

[27] A. N. Pedersen, M. Borup, A. Brink-Kjaer, L. E. Christiansen en P. S. Mikkelsen, „Living and Prototyping Digital Twins for Urban Water Systems: Towards Multi-Purpose Value Creation Using Models and Sensors," *Water,* vol. 13, nr. 5, p. 592, 2021.

[28] W. Sarni, C. White, R. Webb, K. Cross en R. Glotzbach, „Digital Water: Industry leaders chart the transformation journey," International Water Association, London, United Kingdom, 2019.

[29] A. Murillo, R. Taormina, N. Tippenhauer en S. Galelli, „Co-Simulating Physical Processes and Network Data for High-Fidelity Cyber-Security Experiments," in *Sixth Annual Industrial Control System Security (ICSS) Workshop*, New York, NY, USA, 2021.

[30] Wikipedia-bijdragers, „Ijkdijk," Wikipedia, de vrije encyclopedie, 02 03 2022. [Online]. Available: https://nl.wikipedia.org/wiki/IJkdijk. [Geopend 04 2023].

[31] W. Zomer, „New tests IJkdijk: dike breaches predictable with new sensor systems," IJkdijk Foundation, 13 09 2012. [Online]. Available: https://www.dutchwatersector.com/news/new-tests-ijkdijk-dike-breaches-predictable-with-new-sensor-systems. [Geopend 04 2023].

[32] M. Blauw en R. Pot, „Groeifondsvoorstel: Kennis en innovatieprogramma Digital Twins for Dutch Deltas and Infrastructure Alliance (3DINA)," Deltares, 26 April 2021. [Online]. Available: https://www.deltares.nl/nieuws/groeifondsvoorstel-kennis-en-innovatieprogramma-digital-twin-nl-infra-en-ondergrond. [Geopend 04 2023].

[33] G. Burgers, „Programmalijn Digital Dijkmonitoring," Digishape, [Online]. Available: https://www.digishape.nl/programma/dijkmonitoring. [Geopend 04 2023].

[34] „InterTwin," European Union Horizon Europe Programme, [Online]. Available: https://www.intertwin.eu/. [Geopend 04 2023].

[35] „Roadmap Digital Twins," Rijkswaterstaat, 26 3 2021. [Online]. Available: https://rwsinnoveert.nl/focuspunten/data-iv/digital-twins/. [Geopend 4 2023].

[36] J. Wijers, G. Elbersen, A. Koelewijn en N. Pals, „Macrostabiliteit IJkdijk: Sensor- en meettechnologie," Rijkswaterstaat, 2009.

[37] „Totaallijst Dijkmonitoring," Kennisplatform Dijkmonitoring, [Online]. Available: http://www.dijkmonitoring.nl/projecten/totaallijst/. [Geopend 04 2023].

[38] „Dijkinformatie voor beheer en versterking," Kennisplatform Dijkmonitoring, [Online]. Available: https://www.dijkmonitoring.nl/. [Geopend 04 2023].

[39] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou en M. A. Ferrag, „Cyber Ranges and TestBeds for Education, Training, and Research," *Applied Sciences,* vol. 11, 2021.

[40] P. Pernik, „Improving Cyber Security: NATO and the EU," September 2014.

[41] M. o. D. o. Estonia, „CR14 - Multiverse of cyber ranges," Ministry of Defence of Estonia, [Online]. Available: https://www.cr14.ee/. [Geopend 20 2 2023].

[42] „TU Delft's Control Room of the Future maakt elektriciteitsnet digitaal weerbaar," TU Delft, 16 05 2022. [Online]. Available: https://www.tudelft.nl/2022/tu-delft/tu-delfts-control-room-of-the-future-maakt-elektriciteitsnet-digitaal-weerbaar. [Geopend 04 03 2023].

[43] RHEA, „Next Generation Cyber-Range Services," RHEA group, 2021. [Online]. Available: https://www.rheagroup.com/wp-content/uploads/2021/06/RHEA-Group-CITEF-brochure-online-English.pdf. [Geopend 4 03 2023].

[44] AIrbus, „CyberRange - An advanced simulation solution," AIRBUS, [Online]. Available: https://www.cyber.airbus.com/cyberrange/. [Geopend 20 3 2023].

[45] M. Leitner, M. Frank, W. Hotwagner, G. Langner, O. Maurhart, T. Pahi, L. Reuter, F. Skopik, P. Smith en M. Warum, „AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research," in *Proceedings of the European Interdisciplinary Cybersecurity Conference*, New York, NY, USA, 2021.

[46] „AIT Cyber Range," [Online]. Available: https://cyberrange.at/. [Geopend 23 2 2023].

[47] M. Leitner, M. Frank, G. Langner, M. Landauer, F. Skopik, P. Smith, B. Akhras, W. Hotwagner, S. Kucek, T. Pahi, L. Reuter en M. Warum, „Enabling exercises, education and research with a comprehensive cyber range," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA),* vol. 4, December 2021.

[48] M. Kianpour, S. Kowalski, E. Zoto, C. Frantz en H. Øverby, „Designing Serious Games for Cyber Ranges: A Socio-technical Approach," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2019.

[49] „KYPO Cyber Range Platform,” [Online]. Available: https://www.concordia-h2020.eu/kypo-cyber-range/. [Geopend 23 04 2023].

[50] J. Vykopal, P. Celeda, P. Seda, V. Svábenský en D. Tovarnák, „Scalable Learning Environments for Teaching Cybersecurity Hands-on,” *CoRR,* vol. abs/2110.10004, 2021.

[51] P. Empl en G. Pernul, „Digital-Twin-Based Security Analytics for the Internet of Things,” *Information,* vol. 14, nr. 95, 2023.

[52] D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal en H. Janicke, „Digital Twins and Cyber Security – solution or challenge?,” in *6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Preveza, Greece, 2021.

[53] M. Frackiewicz, „Digital Twin for Manufacturing for Cybersecurity and Threat Detection,” 27 March 2023. [Online]. Available: https://ts2.space/en/digital-twin-for-manufacturing-for-cybersecurity-and-threat-detection/. [Geopend 2 May 2023].

[54] A. Pokhrel, V. Katta en R. Colomo-Palacios, „Digital Twin for Cybersecurity Incident Prediction: A Multivocal,” in *Proceedings of IEEE/ACM 42nd International Conference on Software Engineering Workshops (ICSEW'20)*, Seoul, Republic of Korea, 2020.

[55] M. Eckhart en A. Ekelhart, „A Specification-based State Replication Approach for Digital Twins,” in *CPS-SPC '18: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, 2018.

[56] M. Dietz, M. Vielberth en G. Pernul, „Integrating digital twin security simulations in the security operations center,” in *ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020.

[57] D. Nikolopoulos, G. Moraitis, D. Bouziotas en A. Lykou, „Cyber-Physical Stress-Testing Platform for Water Distribution Networks,” *Journal of Environmental Engineering,* vol. 146, nr. 7, 2020.

[58] https://www.nen.nl/normcommissie-internet-of-things, „nen,” [Online]. Available: https://www.nen.nl/normcommissie-internet-of-things. [Geopend 05 06 2023].

[59] „ISO/IEC JTC 1/SC 41 - Internet of Things and Digital Twin,” [Online]. Available: https://www.iec.ch/ords/f?p=103:14:602629840144510::::FSP_ORG_ID,FSP_LANG_ID:27186,25. [Geopend 05 06 2023].

[60] „NIS2 Directive,” [Online]. Available: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555#d1e3342-80-1.

[61] „Wikipedia Nederlands OTAP,” [Online]. Available: https://nl.wikipedia.org/wiki/OTAP.

[62] „Wikipedia Engels DTAP,” [Online]. Available: https://en.wikipedia.org/wiki/Development,_testing,_acceptance_and_production.

[63] „Cyber Resilience Act: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020,” [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[64] Q. Lu, X. Xie, A. K. Parlikad en J. M. Schooling, „Digital twin-enabled anomaly detection for built asset monitoring in operation and maintenance,” *Automation in Construction,* vol. 118, p. 103277, 2020.

[65] A. Hassanzadeh, A. Rasekh, S. Galelli, M. Aghashahi, R. Taormina, A. Ostfeld en M. K. Banks, „A Review of Cybersecurity Incidents in the Water Sector,” *CoRR,* vol. abs/2001.11144, 2020.

[66] B. Williams, M. Soulet en A. Siraj, „A Taxonomy of Cyber Attacks in Smart Manufacturing Systems," in *6th EAI International Conference on Management of Manufacturing Systems*, Cham, 2023.

[67] J. Cervini, A. Rubin en L. Watkins, „Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack," *17th International Conference on Cyber Warfare and Security,* March 2022.

[68] M. Vielberth, M. Glas, M. Dietz, S. Karagiannis, E. Magkos en G. Pernul, „A Digital Twin-Based Cyber Range for SOC Analysts," in *Data and Applications Security and Privacy XXXV: 35th Annual IFIP WG 11.3 Conference, DBSec 2021, Calgary, Canada, July 19–20, 2021, Proceedings*, Berlin, 2021.

[69] T. Miller, A. Staves, S. Maesschalck, M. Sturdee en B. Green, „Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems," *International Journal of Critical Infrastructure Protection,* vol. 35, p. 100464, 2021.

[70] V. Damjanovic-Behrendt, „A Digital Twin Architecture for Security, Privacy and Safety," 24 October 2018. [Online]. Available: https://ercim-news.ercim.eu/en115/special/2103-a-digital-twin-architecture-for-security-privacy-and-safety. [Geopend 24 April 2023].

[71] S. Guida, „Digital Water: Operational digital twins in the urban water sector," 10 March 2021. [Online]. Available: https://iwa-network.org/publications/operational-digital-twins-in-the-urban-water-sector-case-studies/. [Geopend 28 April 2023].

[72] C. A. Bonilla, A. Zanfei, B. Brentan, I. Montalvo en J. Izquierdo, „A Digital Twin of a Water Distribution System by Using Graph Convolutional Networks for Pump Speed-Based State Estimation," *Water,* vol. 14, nr. 4, 2022.

[73] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, A. Ostfeld, D. G. Eliades, M. Aghashahi, R. Sundararajan, M. Pourahmadi, M. K. Banks, B. M. Brentan, E. Campbell, G. Lima, D. Manzi, D. Ayala-Cabrera, M. Herrera, I. Montalvo, J. Izquierdo, E. Luvizotto, S. E. Chandy, A. Rasekh, Z. A. Barker, B. Campbell, M. E. Shafiee, M. Giacomoni, N. Gatsis, A. Taha, A. A. Abokifa, K. Haddad, C. S. Lo, P. Biswas, M. F. K. Pasha, B. Kc, S. L. Somasundaram, M. Housh en Z. Ohar, „Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks," *Journal of Water Resources Planning and Management,* vol. 144, p. 04018048, 2018.

[74] SUTD Itrust , „SWaT Background," [Online]. Available: https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs_swat/. [Geopend 24 04 2023].

[75] SUTD Itrust, „Wadi Background," [Online]. Available: https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs_wadi/. [Geopend 24 04 2023].

[76] PompNL, "De digitale twin van een drinkwaterproductiebedrijf," [Online]. Available: https://www.pompnl.nl/nieuws/de-digital-twin-van-een-drinkwaterproductiebedrijf/. [Geopend 28.03.2023].

[77] A. Heinsbroek, Vitens, "Intelligente drinkwaterzuivering. SLIMM project." [Online]. Available: https://www.waternetwerk.nl/images/knw/2111-WIT-Digital-Twins-Vitens-AH.pdf. [Geopend 28.03.2023].

[78] https://www.digitaltwinhub.org/post/digital-twin-modelling-guides-sydney-water-project-delivery [Geopend 03 2023].

[79] Rhea Group, [Online]. Available: https://www.rheagroup.com/servicessolutions/security/cybersecurity/cyber-range/. [Geopend 03 2023].

Bijlage A

Internationale Cyberincidenten in de Watersector

In deze bijlage wordt een aantal cybersecurity-incidenten in de watersector beschreven. Het zijn internationale incidenten die in wetenschappelijke tijdschriften of (online) media zijn beschreven.

De publicatie van Hassanzadeh et al. [10], getiteld: A Review of Cybersecurity Incidents in the Watersector, biedt een overzicht van 15 gedocumenteerde en openbaar gemaakte cyberincidenten in de watersector gedurende de periode van 2000 tot en met mei 2019. In de publicatie van Miller et al. [11], Looking Back to Look Forward: Lessons Learned from Cyber Attacks on Industrial Control Systems, kiezen de onderzoekers een andere benadering en wordt er in breder perspectief gekeken naar cyberaanvallen op industriële controlesystemen (ICS) en kritieke infrastructuur in het algemeen. In de literatuursurvey worden in totaal 20 aanvallen op industriële controlesystemen gedocumenteerd over een periode van 1988 tot en met juni 2020. Van deze 20 gedocumenteerde incidenten zijn er vijf gerapporteerd als cyberincidenten die overlappen of verband houden met de watersector. In het licht van de diversiteit aan cyberincidenten in de watersector worden vijf verschillende aanvallen belicht om de lezer inzicht te verschaffen.

In 2013 kregen hackers toegang tot de Bowman Avenue Dam in de Verenigde Staten. De hydraulische dam die gebruikt wordt voor de beheersing van overstromingen kon op afstand worden gestuurd doordat hackers zich toegang hadden verschaft tot het interne SCADA-netwerk dat verantwoordelijk is voor de besturing van de dam. Via de aanval konden de hackers informatie inzien over het waterniveau, temperatuur en de stand van de sluisdeur. Hackers slaagden erin om via een verkenningstechniek toegang te krijgen tot een kwetsbare webapplicatie. Deze techniek (Google Dorking) maakt gebruik van speciale zoekopdrachten op Google en openbare informatie om specifieke gegevens te achterhalen. De aanvallers maakten gebruik van een PC binnen het netwerk van de Dam om zo het controlenetwerk te bereiken. Doordat het controlenetwerk op het moment van de hack enkel bezig was met gegevensverzameling, waren de hackers niet in staat om controle uit te oefenen over de dam en de sluisdeuren.

In 2016, werd er door een Amerikaans cybersecurity-bedrijf een veiligheidsbeoordeling uitgevoerd op een Amerikaans waterbedrijf[12]. De securitybeoordeling bracht een aantal risicovolle kwetsbaarheden aan het licht, zoals een grote afhankelijkheid van voornamelijk verouderde hard- en software. Deze verouderde systemen hadden de taak om kritieke waterprocessen te besturen en te regelen, waaronder de klep- en drukbediening. Nadat de kritieke kwetsbaarheden waren ontdekt, werd er een volledig incident response- en

[12] Anoniem waterbedrijf.

onderzoeksplan uitgevoerd. Dit onthulde kwaadwillend netwerkverkeer tussen het normale netwerkverkeer van het waterbedrijf. Het kwaadwillende netwerkverkeer was dan ook bestemd voor IP-adressen die geassocieerd werden met statelijk gesponserde hacktivisten. Na een analyse van het voorval bleek dat er een directe verbinding was tussen de met internet verbonden betalingsserver en het OT-domain. De hackers konden door exploitatie van een betalingsserver vrij gemakkelijk binnendringen op het OT-netwerk. Dit resulteerde in de manipulatie van de chemische processen, klep- en drukregeling, en de exfiltratie van kritieke data. Verder liet een evaluatie van het incident zien dat als de aanvallers meer kennis hadden gehad van de OT- en IT-systemen van het nutsbedrijf, of als de beveiligingsbeoordeling niet had plaatsgevonden, dit ernstige gevolgen had kunnen hebben. De aanwezigheid van verouderde hard- en software maakte het de aanvallers relatief gemakkelijk om zich (na binnenkomst) door het netwerk te verplaatsen.

In 2017 kreeg een regionaal waterbedrijf in het Verenigd Koninkrijk van verschillende klanten te horen dat hun online accountgegevens gewijzigd zouden zijn. Na het opnieuw instellen van de klantgegevens kwam aan het licht dat verschillende geregistreerde bankrekeningen ook gewijzigd waren. Terugbetalingen aan klanten zouden op deze manier terecht komen op frauduleuze bankrekeningen. De aanvallers waren in staat om via deze sluwe manier een totaal van bijna £500 000 buit te maken. Via rekeningen in Dubai en de Bahama's werden vervolgens Bitcoins gekocht die daarna via zogenoemde bitcoin mixers werden weggesluisd. Na een grondige analyse van het incident kon worden vastgesteld dat een medewerker toegang had gehad tot de diverse rekeningnummers die vervolgens waren gewijzigd in frauduleuze rekeningnummers. Ondanks het gebruik van gegevensverwijderingssoftware door de werknemer bleek uit talrijke e-mailberichten met andere criminelen dat de werknemer contact had gehad over de rekeningen die betrokken waren bij de frauduleuze transacties. De werknemer nam foto's van rekeninggegevens en stuurde deze naar zijn criminele assistent. Deze aanval lijkt dan ook een klassiek voorbeeld van een zo genoemde insider threat.

Op 21 januari 2018 heeft er zich ook een cyberincident voorgedaan bij een Europees waterbedrijf. Na het inhuren van het cybersecurity bedrijf Rapidflow werden een heel aantal connecties gedetecteerd naar externe IP-adressen die verdacht gedrag lieten zien. Nader onderzoek liet zien dat de IP-adressen waarnaar de verdachte connecties werden gemaakt onderdeel uitmaakte Crypto Mining Pool specifiek voor het mijnen van Monero-cryptomunten, veelal gebruikt in criminele online transacties. Deze connecties werd geïnitieerd door crypto-mining malware dat binnen het OT-netwerk van het waterleidingsbedrijf aanwezig was. Evaluatie toonde bij dit incident aan dat er door de malware geen verdere pogingen was gedaan om de configuratie van de OT-omgeving te manipuleren, en dat er geen kwaadwillende instructies waren verstuurd in het netwerk wat had kunnen leiden tot schade of impact. Volgens de onderzoekers is dit incident vermoedelijk het eerste bekende geval van een zogenoemde "cryptojacking"-aanval, die door middel van ongeautoriseerd gebruik computerbronnen gebruikt om cryptomunten te mijnen. Dit soort aanvallen kan leiden tot hoog processorgebruik met oververhitting van apparatuur tot gevolg, verdacht netwerkverkeer, en trage reactietijden wat in OT-omgevingen tot gevaarlijke situaties en schade kan leiden.

Op 24 april 2020 werden volgens Israëlische autoriteiten verschillende drink- en afvalwaterfaciliteiten aangevallen op het eigen grondgebied. De aanvallers richtten zich op de PLC's die verantwoordelijk waren voor de aansturing van kleppen die aanwezig waren in de betreffende installaties. Dit leidde er toe dat Israëls Nationale Cyber Directoraat een waarschuwing uitbracht om wachtwoorden van op internet aangesloten apparaten zo spoedig mogelijk te veranderen, software van ICS te updaten, en blootstelling van dit soort

apparaten aan het internet te verkleinen. Volgens de Israëlische waterautoriteit was er door de aanval verder geen schade toegebracht.

Bijlage B

Resultaten Menti-meter van eindpresentatie

De resultaten van dit onderzoek zijn op 19 juni 2023 gepresenteerd aan experts bij het Ministerie I&W en vertegenwoordigers uit de watersector. Tijdens de presentatie is het publiek op een interactieve manier via Menti-meter bevraagd naar hun bevindingen ten opzichte van de resultaten van dit onderzoek, in het bijzonder naar hun mening over de kansen zoals beschreven in hoofdstuk 6. Deze bijlage bevat de resultaten van de Menti-meter uitvraag.

De vragen die het publiek voorgelegd zijn:

Vraag 1. Wat mist er nu aan instrumenten in de cybertoolbox van de watersector om cyberweerbaarder te worden? Antwoorden van de deelnemers zijn visueel weergegeven in onderstaande word-cloud:

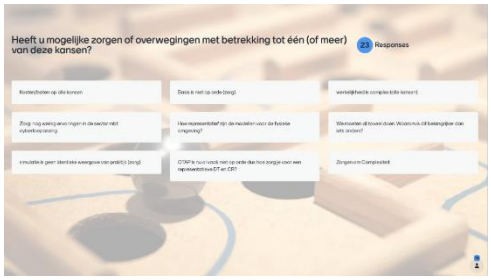
Vraag 2. Wat zijn mogelijke randvoorwaarden om Cyber Ranges in te kunnen zetten? Antwoorden van de deelnemers zijn visueel weergegeven in onderstaande word-cloud:

Vraag 3. Wat zijn mogelijke randvoorwaarden om Digital Twins in te kunnen zetten? Antwoorden van de deelnemers zijn visueel weergegeven in onderstaande word-cloud:

Vraag 4. Welke van de genoemde kansen vindt u het meest relevant en waardevol voor de watersector? De deelnemers hebben op deze vraag hun stem gegeven, welke te zien zijn in de getallen in de zes kansen.

Vraag 5. Heeft u mogelijke zorgen of overwegingen met betrekking tot één (of meer) van deze kansen? De deelnemers hebben de volgende antwoorden gegeven:

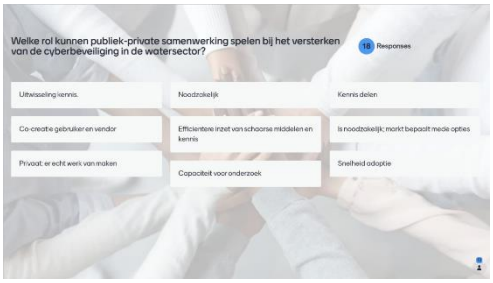
- Kosten/baten op alle kansen
- Basis is niet op orde (zorg)
- werkelijkheid is complex (alle kansen)
- Zorg: nog weinig ervaringen in de sector m.b.t. cybertoepassing
- Hoe representatief zijn de modellen voor de fysieke omgeving?
- We moeten al zoveel doen. Waarom is dit belangrijker dan iets anders?
- simulatie is geen identieke weergave van praktijk (zorg)
- OTAP is nu al vaak niet op orde dus hoe zorg je voor een representatieve DT en CR?
- Zorgen om Complexiteit
- Kramp bij bestuurders. Wegens €€€
- Verschillen in volwassenheidsniveau en daarmee andere behoeften.
- Nog ontbrekende kans: CR inzetten als basis voor OTAP m.b.t. security updates / patch testing / applicatie updates.
- Ik zie een kans door te sturen met DT
- En introduceer hiermee een nieuw of extra risico"
- Haalbaarheid van het opzetten van een van deze kansen die ook betrouwbare resultaten levert. Desondanks de issue met capaciteit, zal het lastig zijn om een 1:1 copy te maken
- Onvoldoende overzicht in landschap en externe digitale afhankelijkheden om het aanvalslandschap voldoende vergelijken af te beelden
- Helpt met bewustwording
- interferentie IT / OT in werkelijkheid
- Overweging: Hoe snel kunnen we dit inzetten? En wat kost het dan? Dit is namelijk erg waardevol om verstoringen te verkennen en analyseren!
- Dreigingen zijn van alle dag. Kijk naar topics
- Misbruik door criminelen om hun methodes te testen
- 100% veiligheid is een illusie. Hoe ver ga je door of course organiseer je de keten anders
- monitoring in praktijk nog niet op orde
- Geld. Kunnen we dit samen doen (m.b.v. ministerie)?



Vraag 6. Welke van de genoemde kansen kan ondersteunen om aan wetgeving en richtlijnen (NIS2, CSIR, CSA,..) in de watersector te voldoen? De deelnemers hebben op deze vraag meerdere keer hun stem gegeven, welke te zien zijn in de getallen in de zes kansen.

Vraag 7. Welke rol kunnen publiek-private samenwerking spelen bij het versterken van de cyberbeveiliging in de watersector? De deelnemers hebben de volgende antwoorden gegeven:

- Uitwisseling kennis
- Noodzakelijk
- Kennis delen
- Co-creatie gebruiker en vendor
- Efficientere inzet van schaarse middelen en kennis
- Is noodzakelijk; markt bepaalt mede opties
- Privaat: er echt werk van maken
- Capaciteit voor onderzoek
- Snelheid adoptie
- Kennisdelen
- Gezamenlijk onderzoek en/of platform ontwikkelen.
- Voorkomen versnippering methoden en aanpak.
- Samenwerken
- Kennis, capaciteit delen
- Kennis en kunde delen, versterken leveranciers relatie
- voorwaarde: elkaars belangen respecteren
- Walk the talk. Dus niet alleen in de brochure veiligheid
- Geen idee: maar het is relatief overzichtelijk met spelers dus samenwerking zou makkelijk moeten zijn....



Vraag 8. Welke voorbeelden van succesvolle publiek-private samenwerkingsinitiatieven in de watersector zijn er? Antwoorden van de deelnemers zijn visueel weergegeven in onderstaande word-cloud:

Defence, Safety & Security

Oude Waalsdorperweg 63
2597 AK Den Haag
www.tno.nl

TNO innovation for life