TEKNISKE OG KRIMINOLOGISKE PERSPEKTIVER PÅ CYBERANGREB MOD INDUSTRIELLE KONTROLSYSTEMER

Forfatter og studienummer:
Jesper Møller - 20231141

Vejleder: Rasmus Munksgaard
Projektgruppe: gruppe 15

Afleveringsdato: 3. juni 2025
Antal anslag: 119.688

Abstract

Cyberattacks targeting Industrial Control Systems pose significant risks to critical infrastructure, yet they remain underexplored within criminological research, which traditionally focuses on individual motivations and online crime. This study investigates how such cyberattacks differ in terms of technical depth and interprets them through criminological perspectives.

Using cluster analysis based on data from the Mitre Attack framework, the project analyzes 460 documented cyberattacks. The results identify six distinct clusters, some of which share common techniques and targets, while each also displays unique characteristics.

Cluster 1 are defined by the use of remote access and lateral movement between IT and industrial environments. Cluster 2 is dominated by Denial of Service attacks aimed at disrupting data flows and operational processes. Cluster 3 rely heavily on valid credentials to maintain persistent control. Cluster 4 targets low-level system components like Data Gateways. Cluster 5 focuses on human-machine interfaces (HMIs), combining physical and logical exploitation, while cluster 6 is characterized by deep technical manipulation and a wide range of targets. The study highlights the importance of integrating technical insight with criminological interpretation to better understand and respond to specific cyber threats against Industrial Control Systems.

Generativ Artificial Intelligence

I det indeværende projekt er Open AI's ChatGPT blevet brugt til at hjælpe med kodningen af data i programmeringssproget Python. Yderligere er ChatGPT bidraget til oversættelse af tekniske termer fra Mitre Attack.

1.0 Indledning

I 2021 udkom Global Risk Report lavet af World Economic Forum med et estimat på, at cyberangreb vil koste virksomheder og organisationer over 6 billioner USD på verdensplan (Shevchenko et al. 2022). Dette skyldes en større digitalisering i form af cloud computing, blockchain teknologi og internet-of-things enheder (IoT).
En del af disse cyberangreb er rettet mod industrielle kontrolsystemer. Teknologien i disse systemer har skabt nye muligheder for at kriminelle hackere kan udnytte muligheden for at forstyrre eller indsamle informationer i disse systemer. Det kritiske ved sådanne cyberangreb er, at industrielle kontrolsystemer understøtter dele af den kritiske infrastruktur i lande verden over, og det medfører yderligere at cyberangreb i dette domæne kan have kritiske konsekvenser for samfundet omkring sig (Maynard et al. 2020).

I 2024 vurderede Center for Cybersikkerhed i Danmark (CFCS) at truslen for destruktive cyberangreb som værende middel. De tilskriver vurderingen af niveauet med det in mente at, statsstøttede aktører om muligt har kapaciteten, men ikke motivationen på nuværende tidspunkt til at udfører sådanne cyberangreb, og derfor kan trusselsvurderingen hurtigt ændre sig (CFCS, 2024a). Cyberangreb mod industrielle kontrolsystemer er præget af højt teknisk formåen og aktørerne sættes ofte i forbindelse med at være statsstøttede hackere. Historisk set har cyberangreb mod industrielle kontrolsystemer været præget af anonymitet og usikkerhed i forhold til hvem eller hvilke nationer der udfører dem. Ej heller findes der juridiske strafferetlige rammer for udførelsen af denne kriminalitetsform (Tsagourias & Farrell, 2020). Af den grund bliver meget af ansvaret lagt over på enkelte produktudviklere og procesejere i kontrolsystemerne.

I dette felt vil nærværende speciale bidrage til en forståelse af hvordan disse cyberangreb opererer, med henblik på at bidrage til et styrket cyberforsvar hos produktudviklere og procesejere i det industrielle cyber-domæne.

2.0 Cyberangreb i tal.

The European Union Agency for Cybersecurity, herefter ENISA, rapporterede en stigning i cyberangreb fra slutningen af 2023 frem til første halvdel af 2024 (ENISA, 2024). ENISA blev etableret i 2004 med det formål at højne cybersikkerheden for EU's medlemslande gennem policymaking, implementering og afrapportering af cybersikkerhedshændelser. De udgiver hvert år en rapport - "ENISA threat landscape". Der er set en markant stigning i cyberangreb på tværs af EU siden sidste kvartal af 2023. Rapporten er udarbejdet ud af 11.000 offentlige rapporterede sikkerhedshændelser, hvoraf ENISA har identificeret syv primære trusler. Dette er både mod informationsteknologi (IT) og operationel teknologi (OT), som vil blive redegjort for senere. Distributed denial of service-angreb topper listen efterfulgt af ransomware og derefter trusler mod data. Disse angreb vil der blive redegjort for senere i opgaven. Denial of service-angreb har ifølge ENISA set en stigning med 41% siden sidste år. Dette skyldes hovedsageligt geopolitiske konflikter, hvilket også ses i Rusland og Ukraine-konflikten. Stigningen i angrebene i 2023 er fordelt ud på 39 forskellige lande. 73 af angrebene var et produkt af en konflikt, 63 var protester, 12 var på baggrund af eksaminer, fem var på baggrund af et valg og fire var på baggrund naturkatastrofer. Angrebene påvirker ifølge ENISA flere og flere mennesker. 41.3% af de denial of service-angreb man så i 2023 resulterede i konsekvenser for mennesker i én eller flere stater, provinser eller byer. Seks ud af otte angreb mod Ukraine var initieret af Rusland, hvorimod 16 angreb mod Palæstina var initieret af Israel.

OT og herunder industrielle kontrolsystemer understøtter store dele af den kritiske infrastruktur. Med kritisk infrastruktur menes der faciliteter, teknologi, herunder systemer, processer, netværk og aktiver, samt serviceydelser, der er nødvendige for at opretholde eller genoprette samfundsvigtige funktioner (CFCS, 2024b). Sektorerne, som dækker kritisk infrastruktur, er blandt andet Transport og Logistik, Vand og spildevand, Sundhedsvæsenet og Forsvaret (Stouffer et al. 2023). Oprindeligt er industrielle kontrolsystemer designet til at være et lukket miljø. Det vil sige at adgangen til systemer og enheder kun har været tilgængelige fysisk og ikke online, og derfor har der ikke været samme udvikling i angrebene som mod it-systemer. Det har løbende ændret sig gennem tiden (Maynard et al. 2020). I takt med at teknologien er blevet bedre, "snakker" industrielle kontrolsystemer og IT mere sammen, hvilket understøtter arbejdsprocesserne og funktionaliteten i systemerne. Det gør dog også at industrielle kontrolsystemer har en større angrebsflade og at det er nemmere eller mere attraktivt at hacke.

2.1 Cyberangreb mod industrielle kontrolsystemer

I juni 2024 udgav Center for cybersikkerhed, herefter CFCS, deres årlige trusselsvurdering mod Danmark (CFCS, 2024c). En vurdering der bar præg af den sikkerhedspolitiske situation verden står i. Cyber-domænet har ifølge CFCS båret præg af krigen mellem Israel og Hamas samt udviklingen af Ruslands invasion af Ukraine, hvilket kunne ses i vurderingen (CFCS, 2024c). Dette er grundet en øget interesse fra stater i at bruge cyberangreb som et værktøj til aktiv krigsførsel. Specielt metoder som spionage, aktivisme og destruktive cyberangreb er i staters interesse, hvorimod cyberkriminalitet med økonomisk gevinst for øje ikke ses som værende en metode der er i staters interesse i samme grad (CFCS, 2024c). Aktivisme, spionage og destruktive cyberangreb har det til fælles at det ifølge CFCS oftest er politisk eller ideologisk drevet. CFCS's trusselsvurdering og tidligere sete angreb peger på, at økonomisk kriminalitet ikke fokuserer på Industrielle kontrolsystemer, men at det er et større fokus for statsstøttede hackere og aktivister. Der har det seneste år været angreb på danske forsyningsselskaber, der blev ramt af såkaldte ransomware-angreb. Der er her tale om Kalundborg Forsyning, Tønder Forsyning og Fanø Vand. Det er ikke kun i Danmark, der er set cyberangreb mod industrielle kontrolsystemer. Et andet eksempel på dette forekom i slutningen af 2024. Her blev et mindre vandværk hacket af prorussiske aktivister. Det medførte at cirka 450 tusind husstande stod kortvarigt uden vand, mens 50 husstande var uden vand i flere timer (TV2 Nyheder, 2025). I takt med at der er set flere angreb mod industrielle kontrolsystemer er der mere empiri at forske i. Litteraturen begrænser sig dog til et teknisk fokus med det formål at forstå, hvordan aktører får adgang og "bevæger" sig gennem systemerne (Maynard et al. 2020). Yderligere er denne form for cyberangreb ikke arbejdet med som en klassisk kriminologisk problemstilling. Kriminologer har i stedet forsket i cyberkriminalitet i forhold til individers normbrud, og i forhold til at indgå i kriminelle miljøer online (Holt, 2022).

2.2 Problemstilling

Industrien er i stigende grad afhængig af digitale systemer til at styre og understøtte den kritiske infrastruktur. Samtidig ses en stigning i målrettede cyberangreb mod industrielle kontrolsystemer. Disse angreb varierer markant i metode, mål og konsekvens, hvilket gør det vanskeligt at etablere en samlet forståelse af trusselsbilledet (CFCS, 2024c, Maynard et al.

2020, Rid, 2014). Derfor er det vigtigt at undersøge, hvordan forskellige typer af cyberangreb mod industrielle kontrolsystemer adskiller sig fra hinanden.

2.3 Problemformulering

Hvordan adskiller cyberangreb mod industrielle kontrolsystemer sig fra hinanden?

2.4 Projektets relevans

Problemstillingen er relevant at undersøge af flere årsager. Cyberangreb mod industrielle kontrolsystemer er ikke et område, der er berørt som en klassisk kriminologisk problemstilling. Det har som tidligere nævnt været tekniske analyser af tidligere sete angreb, som præger feltets litteratur (Maynard et al. 2020). Det er dog heller ikke et område, der er helt fjernt. Cyberkriminalitet er som disciplin et felt hvor kriminologer i stigende grad har undersøgt individers normbrud i kontekst af en hastigt stigende digitaliseret verden, der placerer gerningsmanden i et transnationalt og anonymt miljø (Holt, 2023). Til forskel fra tidligere forskning i cyberkriminalitet er gerningsmandens motivation ikke økonomisk drevet, men derimod en samfundsmæssig destabilisering, som angreb mod den kritiske infrastruktur potentielt medbringer (CFCS, 2024c). Et kriminologisk perspektiv kan derfor bidrage med et holistisk perspektiv på cyberangreb mod industrielle kontrolsystemer. Dette projekt tilbyder en kategorisering af tidligere sete angreb til gavn for en holistisk forståelse af trusselaktører mod den kritiske infrastruktur samt deres tekniske kapabiliteter.

3.0 Eksisterende forskning

I dette afsnit redegøres der for relevant forskning på området. Dette er for at klarlægge hvilke perspektiver der er relevante for at forstå problemstillingen. Derudover vil der blive redegjort for centrale begreber og eksisterende forskning relateret til cyberkriminalitet, cyberangreb og cyberkrig. Forskningen på området spænder bredt og omfatter både tekniske, kriminologiske og sikkerhedspolitiske tilgange. Inden for cyberkriminalitet fokuseres der blandt andet på organiserede grupper, økonomisk motiverede angreb og det voksende marked for kriminelle ydelser som for eksempel Ransomware-as-a-Service, RaaS. Samtidig er der en stigende

interesse for politisk og ideologisk motiverede aktører som hacktivister, der udfordrer traditionelle forståelser af kriminalitet og protest.

I den mere sikkerhedspolitiske ende af spektret beskæftiger forskningen sig med Advanced Persistent Threats, APT'er, og statslige aktører, som anvender cyberangreb som led i geopolitisk konkurrence og hybrid krigsførsel. Denne mangfoldighed af aktører og motiver nødvendiggør en nuanceret forståelse af cyber-domænet som en kompleks og konfliktfyldt arena, hvor både lovgivning, teknologisk udvikling og internationale relationer spiller en rolle. Ved at inddrage eksisterende forskning kan der opnås et solidt fundament for at analysere og forstå de dynamikker, der kendetegner nutidens cybertrusler mod industrielle kontrolsystemer

3.1 Søgestrategier

For indeværende projekt er der brugt metoden "Snowballing" i forhold til at finde relevant litteratur på området (Wohlin, 2014). Indeværende projekt har taget udgangspunkt i følgende søgemaskiner: Google Scholar, The British Journal of Criminology, The Journal of Cybersecurity. De Keywords der indledningsvist er blevet søgt, er herunder men ikke begrænset til "Operational technology, OT, SCADA, Critical infrastructure, Cyber warfare, Advanced persistent threats" Det er forsøgt at være så specifik i søgningen som muligt.

3.2 Perspektiver på cyberkriminalitet, cyberangreb og cyberkrig

3.2.1 Perspektiver på cyberkriminalitet

Dette afsnit beskriver cyberkriminalitet som begreb. Der er ikke et entydigt begreb, men derimod betragtes cyberkriminalitet som værende et paraplybegreb der favner mange forskellige former for online kriminalitet hvor teknologien mere eller mindre spiller en rolle. Det er væsentligt at være bekendt med forskellige definitioner og skillelinjer for at kunne forholde sig til begrebet cyberkriminalitet.

Cyberkriminalitet bruges til at beskrive forskellige former for online kriminalitet, som inkluderer individer til større organisationer samt statsstøttede spionage mod andre nationer

(Collier et al. 2021). Cyberkriminalitet har en lang historik, og forskningen på området er steget de seneste 20 år som en tværfaglig disciplin for både ingeniører, folk i computer science og kriminologer (Holt, 2023). De to førstnævnte har haft fokus på den tekniske del af cyberkriminalitet. Dette kan ses i forhold til dataindsamling gennem scraping, samt udvikling af tekniske foranstaltninger til at forhindre kompromittering af data (Holt, 2023). Kriminologer har i stedet haft fokus på behavioristiske og miljømæssige faktorer, der indvilliger individer til at begå kriminalitet online. Der er ikke en direkte konsensus om hvilke former for kriminalitet begrebet skal dække over. Et af de spørgsmål der rejses hos kriminologiske forskere er, hvilken rolle eller hvor stor en rolle teknologien spiller før man kan snakke om cyberkriminalitet. Mange former for kriminalitet har en eller anden digital komponent til at udfolde sig, men dens tilstedeværelse er stadig i den fysiske verden.

En af de tidlige og mest brugte typologier for cyberkriminalitet er udarbejdet af David Wall (Viano, 2017). Wall forstår cyberkriminalitet gennem fire overordnede typer: Cyber-trespass, cyber-deception/theft, Cyber-porn/obscenity og Cyber-violence.
Cyber-tresspass som dækker uautoriseret adgang til systemer og netværk. Denne slags cyberkriminalitet dækker over computer hacking, hvor personer bryder uautoriseret ind i systemer med henblik på at stjæle, forstyrre eller udforske/spionere (Viano, 2017).

Cyber-deception/theft omhandler digitale former for svindel, bedrageri og tyveri (Holt, 2023). Dette kan omhandle at stjæle informationer fra organisationer, individer eller virksomheder. Cyber-deception/theft hænger unægteligt sammen med cyber-tresspass idet hackere forsøger at tilgå og stjæle data gennem hacking (Viano, 2017).

Cyber-porn/obscenity omhandler alle former for digitale sexuelle lovovertrædelser (Holt, 2023). Dette indebærer distribution af for eksempel børnepornografisk materiale, men også kommunikation i forhold til pædofili, hvor gerningsmænd forsøger at initiere intime forhold til mindreårige (Viano, 2017).
Cyber-violence omhandler brugen af digitale platforme til mobning, chikane, stalking med mere målrettede mod individer (Holt, 2023). Viano argumenterer for at denne type af cyberkriminalitet ikke kun kan begrænses til ovenstående trusler, men at teknologien her spiller en rolle i forhold til at være et supporterende værktøj til kriminalitet, der overføres til den fysiske verden. Han bruger eksemplet om hvordan kriminelle terrororganisationer bruger

digitale kommunikationstjenester til at rekruttere medlemmer, der efterfølgende kan udøve terror i den fysiske verden (Viano, 2017).

En anden typologi er Vianos, som kan anses for at være mere opsummerende af Walls typologi (Viano, 2017). Vianos typologi forholder sig til 1) almindelig kriminalitet udført med informations- og kommunikationstjenester. Med almindelig kriminalitet mener Viano her bedrageri og forfalskning.
2) Kriminalitet rettet mod funktionaliteten af informations- og kommunikationstjenester som indebære hacking, manipulation af systemer samt ødelæggelse af lageret data.
3) Kriminalitet rettet mod internet specifikke interessenter (web-specifik) som for eksempel identitetstyveri.
Vianos typologier kan bidrage med en nuanceret forståelse af cyberkriminalitet ved at kategorisere den ud fra motiver og handlingstyper, hvilket ikke blot synliggør kompleksiteten i det digitale kriminalitetsbillede, men også peger på nødvendigheden af differentierede forebyggelses- og juridiske strategier.

Jonathan Lusthaus påpeger at internet og netværk skal stå centralt, og ikke afgrænses til at være en del af eller stå i periferien i forhold til udførelsen af den kriminelle handling, før der er tale om cyberkriminalitet (Lusthaus, 2012). Han siger følgende:
"There are a number of alternative approaches taken by different scholars, but one simple and useful definition is cybercrime as the 'Use of computers or other electronic devices via information systems such as organisational networks or the internet to facilitate illegal behaviors'. A sensible definition would also specify that the use of networks or the internet is not tangential og peripheral to the crime, such as mere electronic record or communication"
(Lusthaus 2012, s. 72)

I forlængelse af Lusthaus og med henblik på at konkretisere yderligere kan man tale om forskellige slags cyberkriminalitet. Forskere har ofte den opfattelse, at cyberkriminalitet har et højt teknisk niveau og kræver avanceret kompetencer. Sandheden er dog at dette ikke altid er tilfældet. Der kan differentieres mellem to forskellige former for cyberkriminalitet, nemlig cyber-dependent crimes og cyber-enabled crimes (Moneva et al. 2023). Cyber-dependent crimes har en mere teknisk karakter, hvor man bruger computere til at hacke andre computere. Dette kræver en netværksforbindelse og derfor har cyber-dependent crimes ikke

eksisteret før internettet. Kriminalitetsformen i cyber-dependent crimes er hacking, malware-infektioner, Distributed-denial of service-angreb med mere.
Cyber-enabled crime er kriminalitet, der eksisterede før internettet, men som på baggrund af teknologiens udvikling rykkede over i cyber-domænet. Dette er klassiske kriminalitetsformer som hovedsageligt målretter individer og indebærer blandt andet bedrageri, identitetstyveri og stalking.

Afslutningsvis vidner den eksisterende forskning om, at cyberkriminalitet er et komplekst og dynamisk fænomen, der hverken lader sig entydigt definere eller afgrænse. De mange forskellige typologier fra Walls fire typologier til Vianos mere systematiske skelnen illustrerer, hvordan både handlingstype, teknologisk afhængighed og aktørens motiv spiller en afgørende rolle for, hvordan cyberkriminalitet forstås og klassificeres. Dertil kommer en stigende erkendelse af, at ikke al cyberkriminalitet er teknisk avanceret. Mange former for kriminalitet flytter blot kendte kriminalitetsformer over i digitale rammer og tilpasser sig nye kommunikations- og netværksteknologier. Fælles for forskningen er dog en anerkendelse af internettets og informationssystemernes centrale rolle - ikke blot som værktøj, men som kriminalitetens primære arena.

3.2.2 Perspektiver på cyberangreb

Ovenstående afsnit har bidraget til forståelsen omkring hvad cyberkriminalitet er. I dette afsnit bliver der redegjort for forskellige perspektiver på cyberangreb, og yderligere forskellen på cyberangreb og cyberkriminalitet.

3.2.2.1 Juridiske perspektiver på cyberangreb og cyberkriminalitet

Kigger man på differentiering af cyberkriminalitet og cyberangreb i dansk kontekst, refererer CFCS til cyberkriminalitet som værende IT-kriminalitet begået gennem et cyberangreb (CFCS, 2024b). IT-kriminalitet definerer CFCS som værende kriminalitet ved hjælp af IT, hvor formålet er økonomisk berigelse, der kan opnås på forskellige måder, som for eksempel afpresning, eller bedrageri.
CFCS definerer altså at cyberkriminalitet har det klare formål for aktøren at være økonomisk berigelse. Cyberangreb definerer CFCS som hændelser, hvor en aktør forstyrrer eller forsøger

at opnå uautoriseret adgang til data, systemer, netværk eller tjenester. CFCS differentierer cyberkriminalitet og cyberangreb på baggrund af motivationen hos aktørerne og ikke hvilken slags IT eller angrebsmetode (CFCS, 2024b).

Kigger man på en differentiering af cyberangreb og cyberkriminalitet i et lovgivningsmæssigt perspektiv er Convention on cybercrime, Budapest-konventionen og Net- og informationssikkerheds direktivet 2, NIS 2, to centrale juridiske rammer, der dog adskiller sig i både formål og trusselsforståelse.
Budapest-konventionen, vedtaget af Europarådet i 2001, behandler cyberkriminalitet som et transnationalt strafferetligt problem og har til formål at harmonisere medlemslandenes lovgivning om ulovlig adgang, datamisbrug og computerrelateret svindel (Convention on cybercrime LOV nr. 185). Konventionen retter sig mod individuelle eller organiserede aktører, og lægger vægt på efterforskning, retslig forfølgelse og internationalt samarbejde.

I modsætning hertil har NIS 2, vedtaget af EU i 2022, en sikkerhedspolitisk vinkel, idet det fokuserer på at styrke cybersikkerheden i kritiske sektorer gennem krav om risikostyring, hændelsesrapportering og beredskab (NIS 2-direktivet LOV nr. 2555). Direktivet anerkender eksplicit trusselslandskabets kompleksitet, herunder forekomsten af avancerede og vedvarende trusler, som ofte forbindes med statsstøttede aktører (CFCS, 2024b). Hvor cyberkriminalitet som forbindes med individbaserede, økonomisk motiverede lovovertrædelser kan cyberangreb betegnes som strategisk motiverede angreb mod samfundets kritiske infrastruktur.

3.2.2.2 Differentiering af cyberangreb

Kigger man på litteraturen peger forskere på, at der er visse faldgruber og tendenser, når man snakker om cyberangreb (Singer & Friedmann, 2014). Nemlig at cyberangreb bliver brugt til at beskrive alle former for angreb lige så snart der er en grad af teknologi indblandet:
"Essentially, what people too often do when discussing "Cyberattacks" is bundle a variety of like and unlike activities, simply because they involve Internet-related technology. The parallel would be treating the actions of a prankster with fireworks, a bank robber with a revolver, an insurgent with a roadside bomb, and a state military with a cruise missile as if they were all the same phenomenon simply because their tools all involve the same chemistry" (Singer & Friedmann, 2014 s. 68).

Et cyberangreb kan ifølge US National Research Council defineres som værende:
"deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (Singer & Friedmann 2014, s. 68).
Singer og Friedmann mener at denne definition opsummerer, hvad et cyberangreb er, men at man yderligere kan differentiere cyberangreb hvis man holder dem op mod CIA-triaden (Singer & Friedmann, 2014). CIA-triaden står for Confidentiality, Integrity og Availability. Oversat til dansk er dette systemets fortrolighed, integritet og tilgængelighed, som skal ses som de tre overordnede mål, man forsøger at sikre i sit system.
Angreb mod et systems fortrolighed er et forsøg på at opnå uautoriseret adgang til systemer, for at kunne monitorere, eller stjæle informationer omkring systemet eller personer der er registrerede i systemet. Angreb mod systemets integritet har til formål at ændre data i systemer frem for at stjæle dem. Cyberangreb mod tilgængeligheden af et system eller netværk har til formål at forhindre adgang til systemerne. Dette kan ske gennem at nedlægge en hjemmeside via Denial of Service-angreb (Singer & Friedmann, 2014).

Afslutningsvis kan det konstateres, at skellet mellem cyberkriminalitet og cyberangreb ikke alene beror på de teknologiske metoder, der anvendes, men i høj grad også på aktørernes motivation og den kontekst, hvori handlingerne udføres. Hvor cyberkriminalitet primært er drevet af økonomisk gevinst og relaterer sig til individ- eller gruppebaseret lovovertrædelse, indgår cyberangreb ofte i et bredere strategisk og politisk spil, særligt når de rettes mod samfundskritisk infrastruktur. Denne distinktion understøttes både i den juridiske regulering og i den akademiske litteratur, hvor forskere som Singer og Friedmann advarer imod forsimplede kategoriseringer af cyberangreb. En nuanceret forståelse af begreberne og deres anvendelse er derfor afgørende for at kunne analysere og imødegå de komplekse trusler, der i stigende grad præger det cyber-domænet.

3.2.3 Perspektiver på cyberkrig

I dette afsnit redegøres der for cyberkrig som begreb. Der er ikke entydig begreb og der er ej heller konsensus om, i forhold til hvornår der er tale om cyberkrig, cyberkrigsførsel, eller om der overhovedet bliver brugt cyberangreb i krig (Rid, 2014).

Lige så vel som teknologiens udvikling har skabt muligheder for cyberkriminalitet og cyberangreb, har det på samme måde skabt et nyt domæne i krigsførelse. Der findes forskellige definitioner af cyberkrigsførsel og der er ikke en entydig definition af begrebet (Robinson et al. 2015). Robert Alford definerede cyberkrigsførsel som værende at fremtvinge en nations agenda gennem cyberangreb. Michael Robinson modargumenterer Alfords definition, da han mener at det ikke altid er nationer, der fremtvinger deres agenda (Robinson et al. 2015). Religiøse eller ideologiske ideer som ikke har forbindelse til en nation kan ligeledes inkluderes i begrebet.
Andre definitioner som Jeffrey Carr definerer cyberkrigsførsel som værende at slås uden at slås og vinde uden at "spilde blod", her afgrænser han det til aktive konflikter eller nationer der fremtvinger deres agenda. Robinson modargumenterer dog yderligere her, at Carr's definition ikke tager i betragtning at cyberangreb mod den kritiske infrastruktur kan potentielt koste menneskeliv, og derigennem koste "blod" (Robinson et al. 2015).

En af de markante distinktioner mellem cyberkrigsførsel og traditionel krig er, at cyberkrigsførsel ofte foregår under tærsklen for fysisk krigsførelse som en aktiv konflikt mellem to nationer frembringer. Denne mulighed opstår grundet den anonymitet cyber-domænet muliggøre (Robinson et al. 2015).
Thomas Rid argumenterer for at cyberangreb udført at en nation kan betragtes som cyberkrig når det er udført af en statslig aktør, men ikke cyberkrigsførsel eller krig i traditionel forstand, da det falder uden for den juridiske ramme af en væbnet konflikt. (Rid, 2014).
Robinson understøtter denne pointe, at cyberkrig udøves i en gråzone, da et cyberangreb kan foregå uden for en væbnet konflikt (Robinson et al. 2015). Han omtaler cyberangreb, der bruges som værktøj i cyberkrig, herunder spionage, Distributed denial of service-angreb og sabotage. Dette kan betegnes som værende angreb der kan foretages uden for en aktiv konflikt, men stadig indgå som et strategisk værktøj for nationer i cyberkrig (Robinson).

Som et eksempel på hvordan cyberangreb bruges i en væbnet konflikt, samt deres effektivitet argumenterer Frederik Pedersen og Jeppe Jacobsen at Ruslands invasion af Ukraine aktiverede konventionel krigsførsel i de tre klassiske domæner herunder luft, hav og land, samt cyber-domænet. Denne krig var en af de første konflikter, hvor cyberangreb blev brugt som værktøj og indgik aktivt i militære operationer (Pedersen & Jacobsen, 2024). Det står altså klart at cyberangreb har været en integreret del af konflikten, men effektiviteten af deres

angreb kan der stilles spørgsmål ved. Pedersen og Jacobsen argumenterer for følgende fire grunde til, at Ruslands cyberangreb ikke var en succes mod Ukraine.

For det første viser det sig, at russiske cyberoperationer sjældent havde til formål at skabe fysisk destruktion. I stedet var målet ofte destruktion af data, hvilket begrænser cyberspace's nytte som et egentligt krigsføringsværktøj. Dette understøtter den udbredte antagelse om, at cyberoperationer generelt er dårligt egnede til at forårsage fysisk skade.
For det andet var der mange tilfælde, hvor de ønskede effekter af cyberangrebene udeblev. Dette peger på, at cyberspace muligvis favoriserer forsvar frem for angreb – i modsætning til den ellers dominerende antagelse i litteraturen, som betragter cyberspace som angrebsdomineret.
For det tredje gjorde russiske aktører ofte brug af kendt og genanvendt malware. Dette øgede sandsynligheden for, at angrebene blev opdaget og afværget af defensive mekanismer. Denne tendens bekræfter antagelsen om, at offensive cybervåben er flygtige og hurtigt mister deres effektivitet, medmindre de kontinuerligt videreudvikles – en proces, der både er ressourcekrævende og kompleks.
For det fjerde blev cyberoperationer kun sjældent integreret med konventionelle militære operationer. Dette reducerede deres praktiske nytte i krigsmæssig sammenhæng og bekræfter den eksisterende forståelse af, at en effektiv integration af cyberkapaciteter med andre former for militær magt er vanskelig (Pedersen & Jacobsen, 2024).

To forklaringer fremhæves som centrale for disse begrænsninger. Den første omhandler tid. Cyberoperationer kræver typisk længere planlægning og iscenesættelse end konventionelle angreb og har større usikkerhed omkring deres timede effekter. Denne tidsmæssige diskrepans gør det svært at koordinere cyberoperationer med hurtige konventionelle militæraktioner. Den anden forklaring er økonomisk: Operationer baseret på specialudviklet, målrettet malware er dyre og ressourcekrævende, hvilket gør det uholdbart for selv statslige aktører at opretholde en konstant offensiv cyberkapacitet. Derfor blev genanvendelse af malware hurtigt normen for Rusland, hvilket reducerede effektiviteten af angrebene yderligere (Pedersen & Jacobsen, 2024).

Trods denne generelle tendens til begrænset militær nytte, identificerer analysen dog muligheder hvor cyberoperationer kan have indflydelse på krigsførelsen. Det første er på strategisk niveau, hvor vedvarende cyberangreb mod kritisk infrastruktur og statslige institutioner kan svække modstanderens ressourcer ved at omdirigere opmærksomhed og

kapacitet til cybersikkerhed frem for konventionel forsvar. Det andet er på operationelt og taktisk niveau, særligt i krigens indledende fase. Her kan cyberoperationer, som er forberedt før konflikten, implementeres samtidig med, at krigshandlingerne indledes. Dette øger chancen for integration med konventionelle midler og dermed muligheden for at skabe konkrete taktiske eller operationelle fordele (Pedersen & Jacobsen, 2024).

Afslutningsvis kan det konstateres at Cyberkrig er et omstridt begreb uden klar definition og foregår ofte i en gråzone uden for konventionel krigsførelse. Eksemplet med Ruslands invasion af Ukraine viser, at cyberangreb blev brugt strategisk, men havde begrænset militær effekt på grund af manglende destruktiv kapacitet, genbrug af malware og dårlig integration med fysiske operationer. Trods dette har cyberoperationer potentiel værdi på strategisk og taktisk niveau.

3.3 Aktører i cyber-domænet

I dette afsnit redegøres der for forskellige aktører der opererer i cyber-domænet. Der findes mange forskellige aktører der udgør en trussel. De varierer fra hinanden i forhold til motivation, ressourcer og færdigheder, og det er ikke tilstrækkeligt at samle dem under et synonym som for eksempel "hackere" (Singer & Friedmann, 2014). Kigger man på forskellige angreb kan man udlede at der er forskellige motivationer og aktører bag dem. I dansk kontekst bruger CFCS begrebet 'Aktør' som en paraplybetegnelse for alle hackere, herunder en person eller en gruppe af personer fra en organisation, statslig eller privat entitet (CFCS, 2024b). Dykker man ned i hvilke forskellige aktører der findes skelner CFCS her mellem APT'er, Cyberaktivister, og økonomiske ransomware-grupper. Der vil herunder blive redegjort for disse tre.

3.3.1 Advanced Persistent Threats

APT'er er ofte støttet af staten og udgør en mere strategisk og sofistikeret form for cyberangreb (CFCS, 2024b). Det centrale ved en APT er, at den ikke blot sigter mod hurtig gevinst, men derimod etablerer en vedvarende, skjult tilstedeværelse i et system med henblik på spionage eller sabotage. De udfører sofistikerede former for cyberangreb grundet de ikke skal levere hurtige gevinster og har mange ressourcer da de er støttet af staten. De udgør en væsentlig del af den moderne cybertrussel, som sætter pres på både nationale forsvarsstrukturer (CFCS, 2024b). Ifølge Singer og Friedman betegnes APT'er som

"advanced", fordi de anvender sofistikerede værktøjer og metoder, herunder zero-day exploits som er sårbarheder i allerede kendte software-værktøjer som Microsoft eller Adobe. De er "persistent", idet deres operationer er langstrakte og præget af vedholdenhed. Cyberangreb udført af APT'er ophører ikke nødvendigvis ved første succesfulde kompromittering, men opretholdes og videreudvikles over tid. Endelig udgør de en reel "threat", da deres mål og handlinger ofte har nationale sikkerhedsmæssige implikationer (Singer & Friedmann, 2014).

Singer og Friedman fremhæver, at APT'er primært opererer med politiske, militære eller strategiske formål og ikke med umiddelbar økonomisk gevinst som motiv. Deres mål er typisk kritisk infrastruktur, statslige institutioner, forsvarsrelaterede virksomheder eller teknologiske innovationscentre. APT'ers cyberangreb er karakteriseret ved en flertrinsproces, der inkluderer målrettet informationsindsamling, initiel kompromittering af systemer, etablering af skjult og vedvarende adgang, lateral bevægelse i netværket og til sidst eksfiltration af data eller placering af destruktive komponenter. Deres operationer er ofte usynlige for det kompromitterede systems ejer og kan pågå over måneder eller år (Singer & Friedmann, 2014).

Denne pointe understøttes yderligere af Che Mat, som karakteriseres APT'er ved tre centrale egenskaber: deres tekniske sofistikation, deres vedholdende og adaptive angrebsstrategier, og deres fokus på specifikke højtprofilerede mål herunder kritisk infrastruktur, statslige myndigheder og private virksomheder med adgang til værdifuld information (Che Mat et al. 2023).

Singer og Friedman argumenterer for, at APT'er slører grænsen mellem krig, spionage og kriminalitet i cyber-domænet. Deres tilstedeværelse rejser grundlæggende spørgsmål om, hvordan stater skal forsvare sig i en digital virkelighed, hvor fjendtlig aktivitet ikke nødvendigvis manifesterer sig som konventionel krig, men snarere som en konstant, lavintensiv konflikt præget af infiltration og informationsudvinding. I denne sammenhæng fremstår APT'er som et af de mest komplekse og strategisk betydningsfulde fænomener i cyber-domænet (Singer & Friedmann, 2014).

3.3.2 Cyberaktivister

Individer eller grupper der bruger cyberangreb til at fremme en bestemt dagsorden kaldes ofte "Hacktivister", de sættes ofte i forbindelse med cyberangreb som web-site defacement eller Distributed denial of service-angreb (Romagna & Hout, 2017). Hacktivister bruger cyberangreb til at fremme deres ideologiske eller politiske dagsorden. Romagna dykker ned i hacktivistiske ideologier, og fremhæver fem forskellige principper også kaldet "The hacker ethic": 1. At promovere friheden af information, 2. Mistro til autoriteter og fremme decentralisering, 3. Bedømme hackere ud fra deres færdigheder frem for uddannelse, alder, race eller position, 4. Skabe kunst på computere og 5. Bruge computere til at forbedre livskvaliteten.

De to første punkter understøttes af Gabriella Colemans forskning i hacktivistgruppen Anonymous, som illustrerer, hvordan digitale angreb anvendes som protestform mod statslig censur og undertrykkelse. Et konkret eksempel på denne tilgang var Anonymous' defacement af næsten 500 kinesiske hjemmesider som reaktion på Kinas internetcensur. Her blev forsiderne ændret til budskaber rettet mod den kinesiske befolkning, hvor de advarede om regeringens kontrol med internettet og opfordrede til brug af anonymiserende teknologier som Virtual Private Network, VPN, og The Onion Router, TOR. Denne handling viser, hvordan hacktivistiske angreb ofte ikke handler om økonomisk gevinst, men om at sende politiske budskaber og styrke befolkningers adgang til information (Romagna & Hout, 2017).

3.3.3 Ransomware-grupper

Ransomware-grupper er i dag en af de mest fremtrædende trusler i cyber-domænet. Grupperne opererer typisk med økonomisk berigelse som det primære motiv, og har gennem de seneste år udviklet sig til at være enkeltstående aktører til et større organiseret kriminelt netværk. Et ransomware-angreb består i at inficere offerets systemer med ondsindede software som kryptere data, hvorefter aktøren vil kræve en løsesum for at genoprette data. Opfyldes kravet om løsesum ikke, kan data slettes eller offentliggøres af aktørerne. Denne slags cyberangreb er kendetegnet ved en høj grad af teknisk kompetence. Derfor er det også tit større grupper, man ser udføre denne slags angreb (CFCS 2024c).

Ransomware har i de seneste år oplevet en markant vækst, drevet af udsigten til store økonomiske gevinster og lavere tekniske barrierer for udførelse. Begrebet "ransomware" er

en sammensætning af ordene "ransom" (løsesum) og "malware" (ondsindet software) og betegner en type skadelig kode, der primært er forbundet med økonomiske tab for både privatpersoner og organisationer (Botchkovar et al. 2025).

En væsentlig drivkraft bag den stigende udbredelse af ransomware er udviklingen af Ransomware-as-a-Service (RaaS). Denne forretningsmodel har gjort det muligt for flere aktører at indgå i komplekse afpresningskæder. RaaS leverer færdigudviklede ransomware-værktøjer, som kan tilgås og anvendes af tredjeparter via kriminelle online markedspladser. Disse værktøjer tilbydes typisk via licensaftaler eller abonnementsløsninger, hvilket gør det muligt for teknisk mindre erfarne kriminelle at udføre angreb uden selv at udvikle malwaren. Dermed har RaaS gjort ransomware-angreb mere tilgængelig, samtidig med at den økonomiske risiko er fordelt blandt flere aktører (Botchkovar et al. 2025).

Disse organisatoriske strukturer tyder på tilstedeværelsen af velkoordinerede netværk med kapacitet til at fungere som effektive og vedvarende cyberkriminelle syndikater. Alligevel er der stadig kun begrænset forskning i de interne forbindelser og dynamikker, der findes inden for og mellem disse grupper, hvilket gør det vanskeligt at forstå og bekæmpe dem effektivt på et strategisk niveau (Botchkovar et al. 2025).

4.0 Operationel teknologi

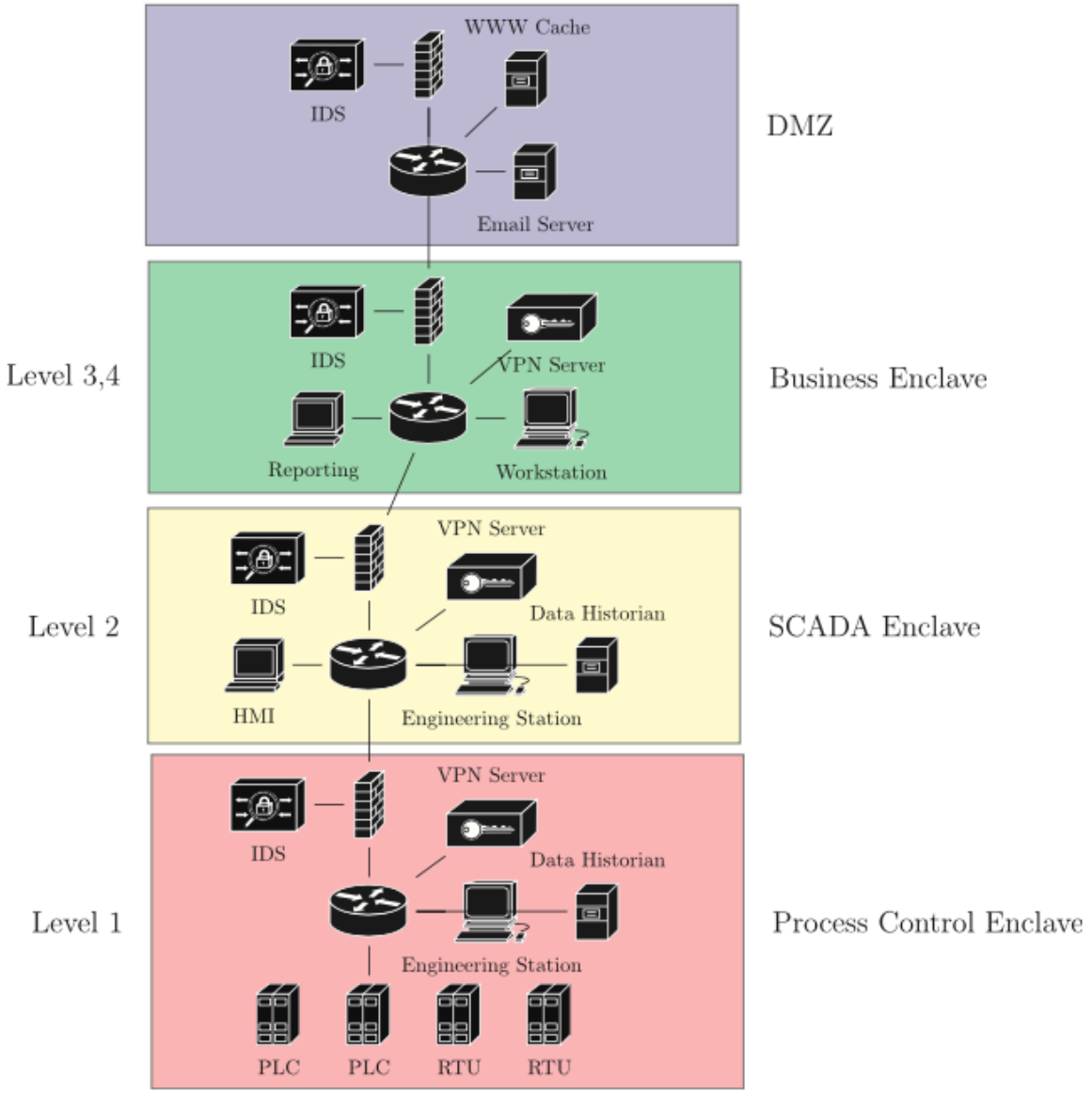
Operationel teknologi omfatter en bred vifte af forskellige systemer og enheder. Nedenstående afsnit vil derfor være redegørende for den typiske opbygning af OT. Det er vigtigt at have en forståelse for hvordan disse systemer er opbygget, da det er omdrejningspunktet som angrebsflade hos de aktører indeværende projekt er bygget op omkring. Designet af OT kan se forskelligt ud hvad end man bruger Supervisory Control and Data Acquisition (SCADA), Distrbuted control systems (DCS) eller Programmable logic controller (PLC) typologien (Stouffer et al. 2023). Idet denne opgaves fokus på industrielle kontrolsystemer afgrænses der til at blive redegjort for SCADA-systemer. SCADA-systemer understøtte meget af den kritiske infrastruktur som der er redegjort for tidligere, og det er yderligere vigtigt her at nævne, at mens mange af sektorerne drives af offentlige myndigheder, er der også mange af systemerne, der er privat ejet og drevet (Stouffer et al. 2023).

4.1 Opbygning af SCADA-systemer

SCADA-systemer bruges primært i industrien og dækker over teknologi, der bruges til realtidsstyring, monitorering og indsamling af data. SCADA-systemer interagerer i det fysiske miljø af en proces. Dette gør også at de er den styrende del, og kan derfor have direkte indvirkning på, hvad der sker i miljøet (Stouffer et al. 2023). Mange SCADA-systemer har et overlap med en eller flere IT-systemer. Dette er med til at højne effektiviteten i arbejdet, men det stiller også yderligere krav til sikkerheden, da det giver en større angrebsflade. IT og SCADA-systemer har hver deres rolle når de udgør et industrielt kontrolsystem. It understøtter data management i forhold til at gøre data tilgængelig gennem applikationer og repositorier, der understøtter forretningen i at kunne behandle data og gøre det tilgængeligt for slutbrugeren. SCADA-systemer er på den anden side et samlet netværk af komponenter, der automatisere ellers fysiske processer i den industrielle proces af arbejdet. Formålet med en større sammenhæng mellem it og SCADA-systemer er distribution og brug af data for begge dele af forretningen (İmamoğlu, 2025)

4.1.1 Sammenhæng mellem it og SCADA-systemer

En visualisering af sammenhængen mellem IT og SCADA-systemer kan ses i figur 1. Her er systemet inddelt ind i fire levels. Level fire er Dimilitiraziation zonen (DMZ). I dette lag er virksomheden disponeret til internettet og her kan bruger tilgå for eksempel virksomheden hjemmeside eller sende mails. Denne zone indeholder Intrusion detection system (IDS) en Domain name server (WWW Cache) og Email server. Level tre er forretnings enklaven, dette er virksomhedens interne netværk, hvor kun medarbejdere har adgang til data til brug for deres daglige arbejde. Level tre indeholder virtual private network (VPN) og arbejdsstationer med mere. I level 2 og 1 har vi SCADA- og proceskontrol enklaverne (Maynard et al. 2025).



Figur 1 - Visualisering af sammenhængen mellem et IT- og SCADA-system inddelt i levels (Maynard et al. 2020)

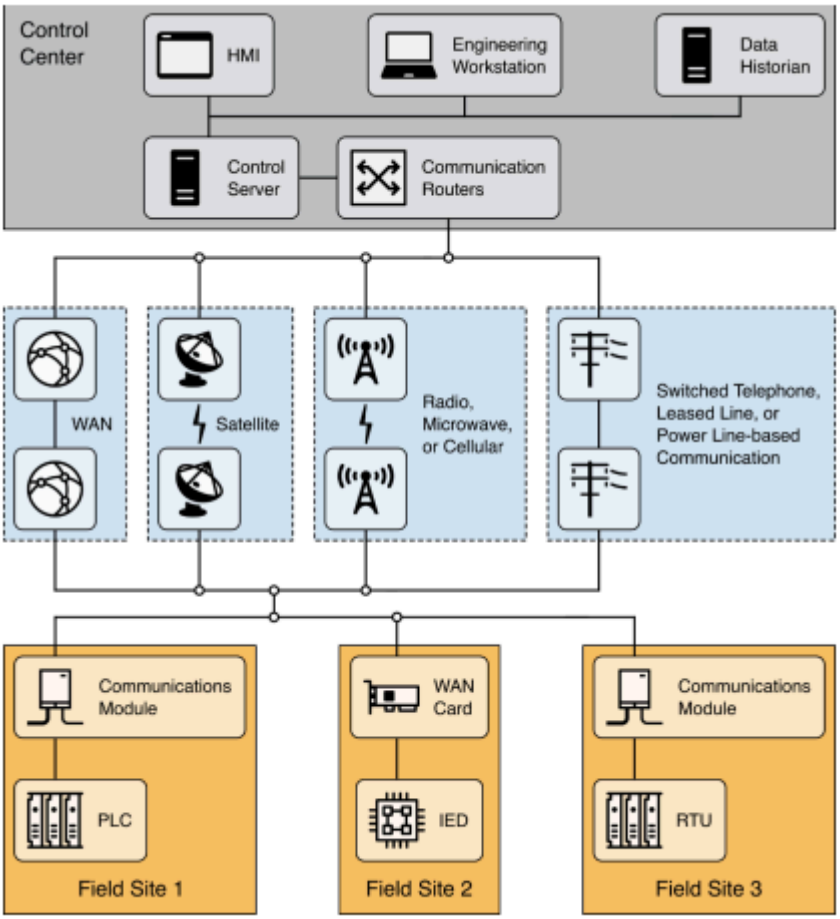
4.1.2 Opbygning af SCADA-systemer

Der vil herunder blive redegjort for SCADA-systemet set i forhold til en anden model, da SCADA-systemet yderligere kan inddeles i flere lag ovenstående oversigt.

SCADA-systemer udgøres af forskellige slags hardware og software, alt efter hvor sofistikerede systemet er. Overordnet set er det opbygget således at man har et kontrolcenter, der huser kontrol servere, kommunikation routere, Human machine interfaces (HMI'er) og Data historians. Komponenterne i kontrolcenteret er sammenkoblet via local area network (LAN) og centrets funktion er indsamling, logging og styring af decentraliseret lokationer,

som kan fjernstyres gennem komponenterne (Stouffer et al. 2023). Nederst i figur 2 ses lokationer som styres gennem kontrolcenteret. Lokationerne er udstyret med kommunikationsmoduler herunder Programmable Logic Controllers (PLC'er), Intelligent Electronic Device (IED'er) og Remote Terminal Units (RTU'er). Komponenterne ude på lokationerne er koblet op på et wide area network (WAN), der gør at information kan transporteres fra decentraliseret lokationer tilbage til kontrolcenteret.

Derudover har de også en fjernadgangs-kapabilitet der gør at operatører kan fjernstyre komponenterne. Dette tillader at operatører kan vedligeholde komponenterne uden fysisk at skulle være til stede. Mellem kontrolcenteret og decentraliseret lokationer har vi forskellige slags fjernkommunikation, der bruges til at transportere information til og fra kontrolcenteret. Fjernkommunikation kan være med radio, cellular og satellit alt efter hvad SCADA-systemet skal understøtte (Stouffer et al. 2023).



Figur 2 - Visualisering af hvordan et SCADA-system er opbygget (Stouffer et al. 2023)

Kigger man nærmere på de specifikke komponenter i ovenstående figur, inkluderer dette kontrolcenter som indeholder Data historian, som har til formål at lager den data der bliver sendt fra de ydre lokationer (Stouffer et al. 2023). Derudover har man HMI'er som er brugergrænseflader hvoraf målingerne kan aflæses, og kommunikationsudstyr herunder, radio, kabler, satellit med mere. Udover dette er de enkelte lokationer udstyret med forskellige slags hardware, der styrer de fysiske processer. RTU'er og PLC'er kontrollere, monitorere sensorer og aktuatorer, som derigennem kan styre den lokale proces.

Kommunikationen mellem disse enheder er understøttet af kommunikationsprotokollen Modbus, som er en af de ældste og mest anvendte kommunikationsprotokoller i SCADA-systemer. Den er enkel og robust, og fungerer ved at etablere en master-slave-kommunikation (Envejskommunikation) mellem en central controller og forskellige enheder som RTU'er og PLC'er. Modbus understøtter både seriel kommunikation (Modbus RTU) og kommunikation over IP-netværk (Modbus TCP/IP), hvilket gør den meget alsidig og let at integrere (DPS Telecom, n.d.).

Control Serveren logger og processer information fra RTU'ens input og output, kommunikationsudstyret tillader at information frit kan flyde mellem kontrol serveren og RTU'en og PLC'en. IEDs fungerer som en sikkerhedskontrol, hvorimod det ovenstående software (RTU og PLC) kun initiere processer inden for acceptable forhold (Stouffer et al. 2023). På samme måde fungerer IEDs i forhold til at stoppe arbejdsprocesser, hvis forholdene ikke er acceptable. IEDs kan kommunikere direkte med kontrol serveren, men er programmeret til at kunne arbejde uden direkte ordre fra kontrolcenteret. IEDs fungerer altså som en sikkerhedsventil, og sker en hændelse fysisk ude på lokationen, kan den by defualt stoppe de igangværende arbejdsprocesser. Denne opbygning gør SCADA-systemer robuste mod fejl med den indlejrede redundans, men dog stadig sårbar for hackerangreb (Stouffer et al. 2023).

4.1.3 Opsamling på Komponenter i SCADA-systemet

Dette afsnit vil kort opsummere, hvad de forskellige servere og komponenter der indgår i SCADA-systemet gør. Det er gennemgået i ovenstående afsnit, men det er vigtigt for læseren

at forstå, hvad deres rolle er i systemet for den videre analyse. Dette afsnit kan bruges til at referere tilbage fra analysen.

Control server

En Control Server er en central computer, der styrer og overvåger automatiserede systemer. Den kører styresystemet og kommunikerer med forskellige tekniske enheder, som styrer maskiner og processer (RTU'er og PLC'er). Til det bruger den særlige kommunikationssprog som Modbus. Control Serveren er også forbundet med et brugergrænsefladen (HMI), så mennesker kan se og styre, hvad der sker i systemet (Stouffer et al. 2023).

Data Historian

En data historian er et system, der opsamler og gemmer data om, hvordan et anlæg eller en proces fungerer, herunder målinger, hændelser, advarsler og alarmer. Systemet bruger en database til at lagre disse oplysninger og tilbyder værktøjer, så man kan analysere dataene. Data historikere bruges ofte af ingeniører, til at få indsigt i, hvordan anlægget kører. Derfor skal de ofte kunne tilgås fra virksomhedens almindelige netværk (Stouffer et al. 2023).

HMI

Et HMI er en brugergrænseflade, som operatører bruger til at overvåge og styre en proces i realtid. Via HMI'et kan man se, hvad der sker i systemet, og justere indstillinger, hvis det er nødvendigt. HMI'en kan være en fysisk skærm eller et kontrolpanel, der sidder fast på en maskine, eller det kan være et program, der kører på en almindelig computer og viser information fra kontrolsystemet (Stouffer et al. 2023).

PLC

En PLC er en specialiseret computer, der bruges til at styre og overvåge maskiner eller processer. Den er bygget op i moduler, så man kan tilpasse den med de funktioner, man har brug for, såsom input/output, kommunikation og behandling af data. PLC'en har forskellige driftsformer (som "Kør", "Stop" eller "Programmering"), der bestemmer, om den skal udføre sine opgaver, eller om man kan ændre dens program. Den bruges altså til at automatisere og sikre, at processer kører korrekt og stabilt (Stouffer et al. 2023).

IED

En IED er en avanceret, specialiseret enhed, som bruges i el-sektoren til at overvåge, beskytte og styre elektriske systemer.

IED'er indsamler målinger og kan selv tage beslutninger og udføre handlinger baseret på indstillinger, man har programmeret på forhånd. De er typisk små indlejrede enheder, som er designet til én bestemt opgave, nemlig at kommunikerer med andre systemer og enheder som controlserveren og RTU'er (Stouffer et al. 2023).

RTU

En RTU er en enhed, der fungerer som et bindeled mellem tekniske enheder (PLC'er og IED'er) og den centrale controlserver. RTU'en har to hovedopgaver: Den sender kommandoer videre fra kontrolsystemet ud til udstyret i marken, og den indsamler data som målinger, hændelser og alarmer fra det udstyr og sender det tilbage til controlserveren. En RTU kan være en specialbygget enhed, et program der kører på en computer, eller software der kører på en PLC. Den er vigtig for at sikre, at information flyder korrekt mellem det centrale system og det udstyr, der styrer de fysiske processer (Stouffer et al. 2023).

4.2 Udfordringer med SCADA-systemer

En af udfordringer med industrielle kontrolsystemer er at de oprindeligt kun har været robuste mod fysisk fjernadgang, det vil sige at holde uønsket udefrakommende væk fra lokationen gennem perimetersikring (Maynard et al. 2020). Grundet deres oprindelige opbygning, var der ikke behov for fjernkommunikation, fordi man havde folk fysisk på lokationen. Med teknologiens udvikling er IT blevet en større del af SCADA-systemers opbygning, hvilket resulterer i at ældre systemer og komponenter i SCADA-systemer bliver sammenhængende med nyere teknologi.
Et eksempel her er, at SCADA-systemer oprindeligt brugte kommunikationsprotokollen Modbus, som tidligere redegjort for, er en kommunikationsprotokol, hvilket stadig ses brugt i SCADA-systemer (Maynard et al. 2020). Selvom teknologien har udviklet sig til at man kan implementere løsninger der ville sikre systemerne bedre, ses der stadig en lang række SCADA-systemer værende outdated i forhold til sikkerheden. Dette skyldes blandt andet

omkostninger i forhold til udskiftning af udstyret eller en generel interesse og viden for sikkerhed hos de driftsansvarlige (Maynard, et al. 2020). Som et resultat af dette er SCADA-systemer modtagelige overfor flere typer af angreb, herunder "Man-in-middle", "command-injections" med mere.

Den større sammenhæng mellem it og SCADA-systemer giver en større angrebsflade for aktører med interesse i at hacke sådanne systemer af (Maynard et al. 2020). En anden udfordring er, at SCADA-systemer er designet til at indsamle og kontrollere aktiver fra forskellige lokationer samlet et sted. De er designet til at overføre information vedr. input og output af processerne fra fjernlokationer tilbage til en operatør, der således kan monitorere og kontrollere den givne proces. SCADA- systemer bliver ofte kaldt "System og Systems" grundet deres indbyrdes afhængighed af hinanden på tværs af sektorer. Et eksempel her er brugen af SCADA-systemer til en centraliseret monitorering af processer og distribution brugt af både elkraft transmission og distributionsnet industrier. Her samler SCADA-systemet både data for offentlig ejet industrier men også private ejet. En hændelse i et system kan derfor have effekt for andre industrier grundet sammenhængen af systemerne. (Stouffer et al. 2023).

4.2.1 Lovgivning og forebyggende arbejde i henhold til SCADA-systemer

Et centralt aspekt af det forebyggende arbejde mod cyberangreb på er udviklingen af regulatoriske rammer, til at bekæmpe cyberkriminalitet (Tsagourias & Farrell, 2020). I denne sammenhæng repræsenterer EU's Cyber Resilience Act (CRA) et markant og strukturelt tiltag, der har til formål at hæve cybersikkerhedsniveauet i hele den digitale forsyningskæde (Cyber Resilience Act, 2022). CRA stiller krav til de produkter og systemer, som udgør den teknologiske infrastruktur. Den er endvidere den første EU-lovgivning, som på systematisk vis pålægger producenter, importører og distributører at indbygge og vedligeholde cybersikkerhed som en integreret del af både hardware og software. Det gælder også produkter, der anvendes i industrielle miljøer herunder komponenter som kontrolsystemer, sensorenheder, kommunikationsgateways og styringssoftware, som alle er centrale i et industrielt kontrolsystem (Cyber Resilience Act, 2022).

Cyber Resilience Act stiller en række konkrete krav til leverandører, som skal sikre, at produkterne er udviklet efter et "security-by-design"- og "security-by-default"-princip. Det

betyder, at produkter skal være designet med indbyggede sikkerhedsmekanismer fra starten og leveres med sikre konfigurationer som standard som for eksempel adgangskontrol, logning, og begrænsning af unødvendige funktioner og porte. Derudover forpligtes leverandører til at overvåge og håndtere sårbarheder løbende, herunder at udstede sikkerhedsopdateringer og patch management i hele produktets levetid. Produkter uden denne løbende vedligeholdelse vil i henhold til CRA ikke længere kunne markedsføres lovligt i EU, hvilket giver incitament til langsigtet sikkerhedsfokus, også efter produktets implementering i kritiske miljøer (Cyber Resilience Act, 2022).

CRA flytter en del af sikkerhedsansvaret opsad, og erkender, at mange sårbarheder opstår allerede i design- og udviklingsfasen som for eksempel ved brug af standardiserede, usikre loginoplysninger, manglende adgangssegmentering eller svag implementering af opdateringsrutiner. Ved at stille krav til, hvordan leverandører dokumenterer og reagerer på kendte sårbarheder, skaber CRA rammerne for en mere ensartet og forpligtende tilgang til cybersikkerhed i hele produktets livscyklus. Derudover indføres der en obligatorisk underretningspligt, hvor alvorlige sårbarheder skal rapporteres til ENISA og nationale myndigheder inden for 24 timer efter opdagelse. Dette er et vigtigt værktøj til at sikre rettidig respons og til at dele viden på tværs af sektorer, hvilket er særligt relevant i kritiske miljøer, hvor angreb kan sprede sig hurtigt og have omfattende konsekvenser.

CRA bruges til at standardisere og styrke sikkerhedsniveauet fra produktionsleddet. Det forebyggende sigte ligger ikke blot i at forhindre enkelte tekniske sårbarheder, men i at fremme en kultur, hvor cybersikkerhed er en integreret og kontinuerlig proces snarere end en engangsindsats. Dette gør CRA til et vigtigt redskab i det bredere forsøg på at begrænse angrebsflader, minimere risikoen for kompromittering og styrke samfundets modstandsdygtighed mod cybertrusler i kritisk infrastruktur.

5.0 Metode og empiri

I dette afsnit vil de designmæssige overvejelser blive behandlet, herunder datagrundlaget, som er data fra Mitre attack's database. Afsnittet vil berøre de begrænsninger data medfører, og endvidere komme ind på den ønskede analysestrategi som er klyngeanalyse, her med fokus på de kvalitetskriterier som afstandsmål og sammenlægning der ligger til grund for

analysen. Yderligere vil begreberne i data blive operationaliseret, således at der er gennemsigtighed af de variable, der er relevante for besvarelse af problemformuleringen. Til sidst i afsnittet vil en kort gennemgang af datahåndteringen blive gennemgået, samt vil etiske overvejelser, der er gjort i forbindelse med projektet blive adresseret.

5.1 Design

I en undersøgelse er det væsentligt at begynde processen med at klarlægge et design, således at det bedst muligt besvarer problemformuleringen (Andersen et al. 2012). Med design menes der en overordnet plan for forskningsprocessen. Dette indebærer at klarlægge hvilke data og og metoder der skal benyttes til at besvare problemformuleringen. I dette projekt er problemformuleringen som tidligere nævnt:

Hvordan adskiller cyberangreb mod industrielle kontrolsystemer sig fra hinanden?

For at besvare problemformuleringen tages der udgangspunkt i Mitre Attacks database og nærmere deres Industrial Control Systems-domæne. Databasen består af et struktureret katalog over kendte cyberangreb målrettet industrielle kontrolsystemer, herunder deres tekniske beskrivelser og tilknyttede aktører (Alexander et al. 2020). Data udgøres af tværsnitsdata, da det består af enkelte kampagner og hvordan de er udført og ikke en udvikling over tid.
Baggrunden for at bruge tværsnitsdata skyldtes at problemformuleringen ikke fordrer en tidsdimension, da det ikke ønskes at undersøge en forandring over tid, men udelukkende at se forskelle mellem cyberangreb. Data indeholder informationer omkring hvordan aktører opererer i praksis, og beskriver specifikke taktikker, teknikker og procedurer, TTP'er, som benyttes i forskellige faser af en kampagne. Studiet er tilrettelagt som værende induktivt, da det ikke ønskes at tage udgangspunkt i eksisterende teori eller at opstille og teste hypoteser. Den empiriske analyse bygger udelukkende på de sammenhænge og mønstre der findes i empirien (Andersen et al. 2012). Til den empiriske analyse bruges metoden klyngeanalyse. Klyngeanalyse betragtes som en grundlæggende metode inden for data mining. Data mining er forsøget på at udtrække interessante mønstre i data (Wu, 2012). Med denne metode er det muligt at identificere, hvordan forskellige cyberangreb adskiller sig fra hinanden baseret på aktørernes adfærd. Metode samt data vil blive uddybet i efterfølgende afsnit.

5.2 Empiri

I ovenstående afsnit blev det begrundet, hvorfor det er relevant at bruge data fra Mitre Attack baseret på problemformuleringen, samt benyttelse af metoden klyngeanalyse. I dette afsnit vil jeg kort redegøre for indsamling af data samt dennes struktur.

Det er væsentligt at pointere at empirien består af sekundære data. Med sekundær data menes der, at det allerede er eksisterende empiri som er indsamlet til andre formål, hvilket stiller krav til at man som forsker overvejer, hvorvidt data møder de kvalitetskriterier, indeværende projekt stiller. Et af disse kriterier er blandt andet at man ikke selv har stået for dataindsamlingen, det er derfor nødvendigt at stille sig kritisk til den data man arbejder med (Clark et al, 2021).

Mitre Attack er udviklet af den amerikanske forskningsorganisation MITRE med det formål at understøtte forståelsen af, hvordan aktører opererer i praksis. Mitre er en amerikansk non-profit organisation, med fokus på at udvikle løsninger i offentlighedens interesse som for eksempel med data fra virkelige hændelser (Mitre, n.d.a). Mitre Attack er en offentligt tilgængelig database over kendte kampagner. Dens styrke som forskningsredskab udspringer af flere kerneegenskaber. For det første skaber Mitre Attack et fælles sprog for trusselsforståelse, hvilket gør det muligt for forskere at sammenligne data og resultater på tværs af studier og organisationer. For det andet bygger Mitre Attack på empiriske observationer fra den virkelige verden, hvilket sikrer, at forskningsresultater, der tager udgangspunkt i databasen, har høj praktisk relevans (Alexander et al. 2020). Derudover opdateres databasen løbende på baggrund af globale bidrag, hvilket sikrer, at den forbliver dynamisk og reflekterer det aktuelle trusselsbillede.

Med henblik på at skabe en forståelse for data er det nødvendigt at gennemgå de forskellige variabler, der skal ligge til grund for analysen. Datasættet fra Mitre Attack er V.17.1. Det er henholdsvis tre datasæt der er blevet sammenfattet til et, herunder “Procedure examples”, “Techniques” og “Assets”. Data er sammenfattet af de forskellige datasæt for at opnå de variable der er relevante for nærværende projekt, som der vil blive redegjort for i projektets operationalisering.

Variablerne efter sammenfatningen består af ‘campaign_id’, ‘technique_name’ og ‘target_name’. Variablen ‘campaign_id’ fungerer som en unik identifikator for hver

kampagne i datasættet. Variablen er baseret på Mitre Attacks officielle struktur, hvor hver dokumenteret kampagne tildeles en unik kode for eksempel C0020 eller C0021 (Alexander et al. 2020). Denne identifikator muliggør en entydig reference til hver kampagne og sikrer, at sammenhørende teknikker og mål korrekt knyttes til den rigtige observation i datasættet. Variablen 'technique_name' omfatter de specifikke angrebsmetoder der er anvendt i en kampagne og beskriver en individuel handling udført af en aktør mod industrielle kontrolsystemer. Variablen 'target_name' omfatter de typer af komponenter, som udgør et industrielt kontrolsystem. Det omfatter som tidligere redegjort for komponenter som for eksempel 'HMI'er', 'PLC'er', 'Data historians' og 'Applikationsservere'.

En kampagne er en samlet mængde aktivitet, der er udført over en bestemt tidsperiode, rettet mod fælles mål og med fælles strategiske eller operationelle formål. Hvis den rapporterede aktivitet ikke har et officielt navn, tildeles den et unikt Campaign ID, ellers benyttes de navne, der fremgår af offentligt tilgængelige kilder. Kampagner bliver, i det omfang det er muligt, koblet til specifikke trusselsgrupper og softwarekomponenter i databasen, baseret på offentlig dokumentation. Kortlægningen af kampagner inkluderer også de teknikker, som er offentligt dokumenteret i forbindelse med den pågældende aktivitet, samt henvisninger til originale kilder. Det er dog vigtigt at bemærke, at listen over teknikker ikke nødvendigvis er udtømmende, men afspejler det udsnit, som er tilgængeligt gennem åbne kilder (Mitre, n.d.-b)

Datasættet repræsenterer således tilsammen cyberangreb gennem en taksonomi, hvor hver kampagne er knyttet til en eller flere teknikker og mål. Disse to dimensioner er observerbare indikatorer på hvordan kampagnerne er struktureret og udført. For at kunne udarbejde en klyngeanalyse af angrebene og dermed besvare problemformuleringen, kræver det at dataen transformeres til en form, der egner sig til kvantitative analyser. Variablerne grupperes pr. kampagner således at datasættet består af en dataframe, hvor hver række svarer til en kampagne og hver kolonne repræsenterer en specifik teknik eller mål. Datastrukturen efter omkodning muliggør således at kunne klynge kombinationen af alle teknikker og mål i hver kampagne. I alt er der 460 observationer, baseret på forskellige kampagner udført mod industrielle kontrolsystemer. Observationer er kombinationen af en teknik brugt mod et mål.

	campaign_id	campaign_name	technique_id	technique_name	tactic	platform	target_id	target_name	target_type
0	C0028	2015 Ukraine Electric Power Attack	T0803	Block Command Message	Inhibit Response Function	NaN	T0803	Control Server	asset
1	C0028	2015 Ukraine Electric Power Attack	T0803	Block Command Message	Inhibit Response Function	NaN	T0803	Field I/O	asset
2	C0028	2015 Ukraine Electric Power Attack	T0803	Block Command Message	Inhibit Response Function	NaN	T0803	Human-Machine Interface (HMI)	asset
3	C0028	2015 Ukraine Electric Power Attack	T0803	Block Command Message	Inhibit Response Function	NaN	T0803	Intelligent Electronic Device (IED)	asset
4	C0028	2015 Ukraine Electric Power Attack	T0803	Block Command Message	Inhibit Response Function	NaN	T0803	Programmable Logic Controller (PLC)	asset

Figur 3 - Udsnit af dataframen der tilvejebringer projektets analyse.

5.3 Operationalisering

For at kunne besvare problemformuleringen om hvordan cyberangreb adskiller sig fra hinanden, er det nødvendigt at operationalisere begreberne således det er muligt at udarbejde en systematisk analyse. Dette afsnit operationaliserer begreberne som bruges i nærværende projekt.

For at undersøge hvordan cyberangreb mod industrielle kontrolsystemer adskiller sig fra hinanden, er det nødvendigt at have målbare enheder der kan give indsigt i dette. En operationalisering er, at definere, hvilke operationer man skal foretage sig for at måle et begreb (Clark et al. 2021). For indeværende projekt er det cyberangreb der skal måles i forhold til hvordan de adskiller sig. Cyberangreb skal for indeværende projekt forstås som værende en sammensætning af en teknik der bliver brugt mod et eller flere mål i et industrielt kontrolsystem. Som tidligere redegjort for bruger indeværende projekt, data fra Mitre Attack, hvorved man kan se hvilke teknikker der er brugt mod hvilke komponenter i en kampagne. Således vil en kampagne for eksempel C0028 - kampagnen mod det Ukrainske elnet i 2015 bestå af flere cyberangreb (se figur 3).

At adskille sig fra noget betyder ifølge den danske ordbog: “være anderledes; være forskellige fra” (Det Danske Sprog- og Litteraturselskab, n.d.). For indeværende projekt

bliver adskillelsen af cyberangreb fortolket ud fra hvilke teknikker og mål de enkelte cyberangreb rammer

For at kunne operationalisere ens koncept, er der ifølge Bryman forskellige måder hvorpå man kan opnå validitet af ens variabler. En af metoderne er at etablere 'Face validity'. Dette indebærer at tage udgangspunkt i, hvad andre eksperter har udarbejdet på området (Clark et al. 2021). CFCS adskiller cyberangreb med henblik på at beskrive deres forskelle, og giver i deres rapport "Et wiper-angrebs anatomi" følgende metode på, hvordan man adskiller cyberangreb fra hinanden. CFCS opdeler et angreb i faser, hvor de kigger på hvad aktøren bruger af teknikker og hvilke mål de rammer, i de forskellige faser af et wiper-angreb. (CFCS, 2024d).

Med refleksionen omkring, hvordan CFCS adskiller cyberangreb fra hinanden, kan det i indeværende projekt argumenteres, at hvis man tager udgangspunkt i angrebenes anvendte teknikker og mål, udgør det et brugbart analytisk koncept til systematisk at differentiere mellem forskellige typer af cyberangreb

5.4 Metode/Analysestrategi

Dette afsnit vil indebære en gennemgang af klyngeanalyse som metodisk værktøj, yderligere vil det blive gennemgå hvordan denne metode bliver brugt i forhold til data fra Mitre Attack, og endvidere komme ind på beslutninger der er taget i forhold til afstandsmål og processen omkring at analysere klyngerne.

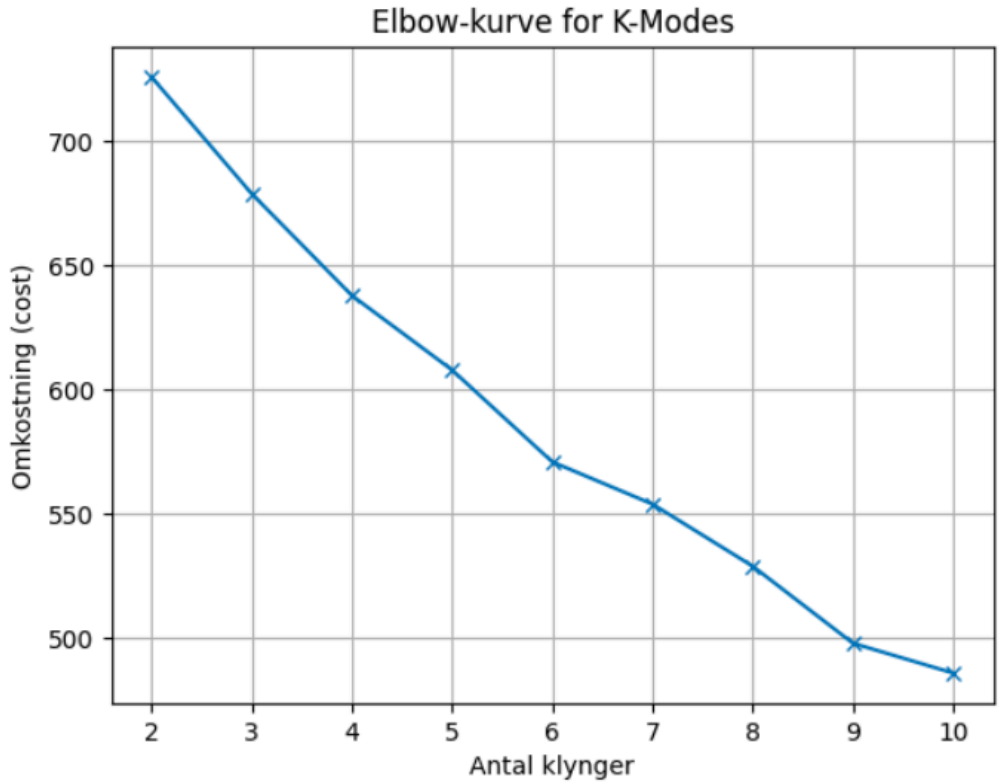
5.4.1 Klyngedannelse

Som nævnt tidligere er klyngeanalyse brugt som metodisk værktøj til at besvare indeværende projekts problemformulering. Der findes en række forskellige måder at klynge sin data på, og det er vigtigt at tilrettelægge sin analytiske tilgang ud fra det spørgsmål, som skal besvares (Andersen et al. 2012). Som nævnt tidligere består datasættet fra Mitre Attack af i alt 460 observationer af cyberangreb. Til dette projekt bruges en klyngeanalyse nærmere K-modes clustering.

K-modes clustering er videreudviklet fra den klassiske K-means metode, hvoraf den er tilpasset til at håndtere kategoriske værdier. K-modes sikrer klynger med høj intern homogenitet og ekstern heterogenitet, idet klyngecentrerne repræsenteres med de mest

hyppige værdier for hver variabel inden for klyngerne (Halkidi et al. 2001). Der er indledningsvist tre forhold, der gør sig gældende ved brugen af K-modes clustering. Det første valg omhandler at man på forhånd skal vælge hvor mange klynger (k) der initieres af algoritmen. K-modes algoritmen blev kørt for værdier af k i intervallet 2 til 11. Valget af intervallet i klyngeanalyse baserer sig primært på overvejelser om fortolkning og praktisk anvendelighed, hvilket understøttes af Maria Halkidi, Giannis Batistakis og Michalis Vazirgiannis. De fremhæver, at validering af klyngeanalyse ikke alene bør bero på matematiske eller statistiske mål, men i lige så høj grad tage højde for anvendelseskontekst og analytisk brugbarhed. I tråd med denne tilgang er det centralt, at antallet af klynger ikke overstiger det punkt, hvor fortolkningen bliver vanskelig eller meningsløs. Valget af et relativt snævert interval, hvor k ikke overstiger 11, er således truffet ud fra hensynet til, at analysens resultater skal kunne anvendes og kommunikeres klart uden at miste overblikket over de strukturer, som identificeres i datasættet. Ifølge forfatterne er dette i overensstemmelse med god praksis i klyngevalidering, hvor meningsfuldhed og praktisk relevans vægtes på linje med teknisk præcision (Halkidi et al. 2001).

Endvidere for klyngeanalysen bliver hver iteration for modellens samlede omkostning beregnet. Denne omkostning er defineret som summen af forskelle mellem hver observation og dens tildelte mode. Ved at visualisere omkostninger som funktion af k blev det muligt at identificere det punkt, hvor yderligere stigninger i antallet af klynger medførte aftagende forbedring, på baggrund heraf blev det optimale antal klynger fastsat til $k = 6$ - altså seks klynger. Antallet af klynger er fastlagt ved anvendelse af Elbow-metoden. Der er herunder indsat en visualisering af Elbow-metoden, hvor man kan se grafen flader ud mellem de to punkter seks og syv.



Figur 4 - Elbow-kurven visualiseret. y-aksen er omkostninger (iterationer) og x-aksen er antal klynger.

Det andet valg er initialiseringen af modes, som er foretaget ved brug af Huang's frekvensbaserede metode (Halkidi et al. 2001). Her udvælges startpunkterne blandt de mest hyppigt forekommende observationer, og efterfølgende modes vælges med maksimal forskel fra de tidligere valgte. Denne tilgang øger konvergensens stabilitet og reducerer risikoen for, at algoritmen konvergerer til et lokalt minimum.

Derudover blev modellen initialiseret fem gange (*n_init = 10*) for at sikre robusthed og finde den bedst mulige klyngedannelse (Halkidi et al. 2001). Yderligere anvender k-modes en simpel uoverensstemmelsesmåling, der tæller antallet af forskellige kategoriværdier mellem to observationer. Efter modelkørslen tildeles hver observation en klynge, og dette output danner grundlag for den efterfølgende klyngeprofilering. Denne fremgangsmåde muliggør en meningsfuld klyngedannelse, der respekterer datasættets kategoriske struktur og samtidig sikrer høj intern kohæsion og ekstern separation – kriterier som ifølge Halkidi udgør centrale målestokke for validiteten af klyngeanalyse.

5.4.2 Analysestrategi

Efter klyngedannelsen vil cyberangrebene være inddelt på baggrund af hvilke teknikker og mål der er brugt til at udføre kampagnerne. Den videre analysestrategi på baggrund af klyngedannelsen, og med henblik på besvarelse af problemformuleringen, vil foregå således at hver klynge vil blive analyseret systematisk med udgangspunkt i de to variable der er klynget på, herunder teknikker og mål. Klyngerne vil blive navngivet ud fra deres karakteristika baseret på variablerne. Den første del af analysen vil foregå overordnet, hvor det på baggrund af klyngernes profil vil blive fortolket med for øje at beskrive cyberangrebenes formål i de enkelte klynger. Dette er på baggrund af hvilke teknikker og mål der ses internt i klyngerne.
Efterfølgende vil klyngerne blive gennemgået i forhold til deres tekniske karakter. Her oversættes Mitre-teknikker til dansk for fortolkningens skyld. Det bliver yderligere beskrevet hvad teknikkerne gør og hvordan de kan bruges. Til sidst i denne del af analysen vil de mål klyngerne rammer internt blive gennemgået. De bliver nærmere beskrevet, hvad deres funktion i systemerne er, og hvordan cyberangrebene kan ramme dem.
Slutteligt vil hver klynge blive fortolket gennem Walls typologier for cyberkriminalitet herunder Cyber-trespass, Cyber-deception/theft, Cyber-pornography/obscenity og Cyber-violence. Denne fortolkning har til formål at koble de tekniske fund med kriminologiske perspektiver og dermed belyse, hvilke former for skade, kontrol eller overtrædelser der karakteriserer de enkelte angrebsformer. Dette giver et bredere blik på, hvordan cyberangreb mod industrielle kontrolsystemer kan placeres inden for eksisterende kategorier af cyberkriminalitet.

Den analytiske tilgang vil bidrage til en nuanceret forståelse af, hvordan cyberangreb mod industrielle kontrolsystemer adskiller sig fra hinanden.

5.5 Datahåndtering

Formålet med dette afsnit er at klarlægge, hvordan datasættet fra Mitre Attack er blevet etableret. Det er yderligere hensigten at have gennemsigtighed gennem processen med kodning her med tanke på hvilke pakker der er blevet brugt til at arbejde med dataen.

Datahånteringen i dette projekt er blevet udarbejdet i programmet Jupyter notebook med programmeringssproget Python 3. Scriptet der er lavet i Python 3 er vedlagt projektet med henblik på gennemsigtighed. Indledningsvist er datasættet sammensat af tre forskellige datasæt der er alle hentet fra Mitre Attacks officielle hjemmeside. Datasættene er hentet med pakken Openpyxl som tillader at trække internet-filer ind i Jupyter notebook. Datasættene er efterfølgende blevet bearbejdet i en Pandas dataframe med pakken Pandas, hvor de tre datasæt er sat sammen via fælles identifikationsnumre kaldet "Campiagn_id". Datasættet er struktureret, således at hver kampagne indeholder hvilke teknikker samt hvilke mål der er brugt af aktørerne. Tæller man alle cyberangreb på tværs af alle kampagnerne i datasættet er der 460 forskellige slags cyberangreb. Denne datahåndtering tillader at udarbejde en K-modes klyngeanalyse, som det for indeværende projekt er udarbejdet med pakken kmodes.kmodes version 0.12.2. Yderligere er afstandsmål foretaget med 'Huang' og Random_state er sat til 42 for analysens gentagelighed. For at udregne det maksimale antal klynger er der visualiseret en graf der viser hvor "knækket" på kurven er. Dette er kaldt elbow-metoden. På baggrund af den kurve er valget om seks klynger foretaget. Yderligere er analysens resultater visualiseret med pakkerne 'Seaborn' og 'PLT'.

Med ovenstående datahåndtering har har der været muligt at indhente og foretage samensætte de variabler der ligger til grund for klyngeanalysen, og derigennem besvarelsen af indeværende projekts problemformulering.

5.6 Etiske overvejelser

Ved anvendelse af data fra Mitre Attack i forskning og analyse bør man overveje en række etiske aspekter, som relaterer sig til forskellige principper herunder utilsigtet skade og vildledning (Clark et al. 2021). I dette afsnit redegøres der for hvilke overvejelser der er gjort i forhold til disse principper i det indeværende projekt.

Etisk vildledning kan opstå, hvis forskere fremstiller data som neutrale, objektive eller fuldstændige, uden at tydeliggøre den kontekst og de antagelser, der ligger bag (Clark et al. 2021). Mitre Attack er en database, hvor udvælgelsen af aktører, teknikker og TTP'er er foretaget af en organisation med tilknytning til vestlige sikkerhedsinteresser (Alexander et al. 2020). Selvom om indeværende projekt ikke direkte berører aktørerne bag cyberangrebene,

kan det hurtigt fremsøges hvilke nationer aktørerne er støttet af, eller formodes at være støttet af. En etisk ansvarlig tilgang indebærer derfor, at man undgår implicit vildledning gennem urefleкteret brug. Indeværende projekt gør ikke brug, eller henleder ikke til at drage konklusioner omkring de aktører der fremgår i indeværende projekt. Den analytiske værdi og de konklusioner der drages forholder sig udelukkende til den tekniske anvendelse af cyberangreb mod industrielle kontrolsystemer. Der henledes derfor ikke til at drage konklusioner der ville kunne føre til overeksponering af specifikke grupper, som igen kan føre til stigmatisering af bestemte nationer eller individer.

En anden etisk overvejelse, der er værd at være opmærksom på, er spørgsmålet om utilsigtet skade (Clark et al., 2021). Når dette projekt gengiver tekniske detaljer om angrebsmetoder, rejser spørgsmålet sig om, hvorvidt sådanne oplysninger potentielt kan udnyttes af ondsindede aktører. Data i projektet er imidlertid baseret på allerede dokumenterede hændelser, hvoraf flere ligger flere år tilbage. Angrebsmetoderne er dermed offentligt kendt og en del af eksisterende trusselsviden. Det vurderes derfor, at projektet ikke bidrager med operative nybrud, men snarere med analytisk strukturering. Ikke desto mindre tages der højde for den etiske balance mellem at styrke forsvarsevnen og at minimere risikoen for at reproducere eller sprede anvendelige teknikker.

6.0 Analyse af klynger

Dette afsnit vil indledningsvist beskrive inddelingen af klynger, i forhold til hvilke der er størst i antal observerede cyberangreb. Yderligere vil afsnittet være beskrivende overfor de forhold der gør sig gældende vedrørende den analytiske konsekvens af at arbejde med komplekst data. Endvidere vil hver klynge blive beskrevet i forhold til deres formål, tekniske sammensætning og blive fortolket ud fra Walls typologier vedrørende cyberkrimianlitet.

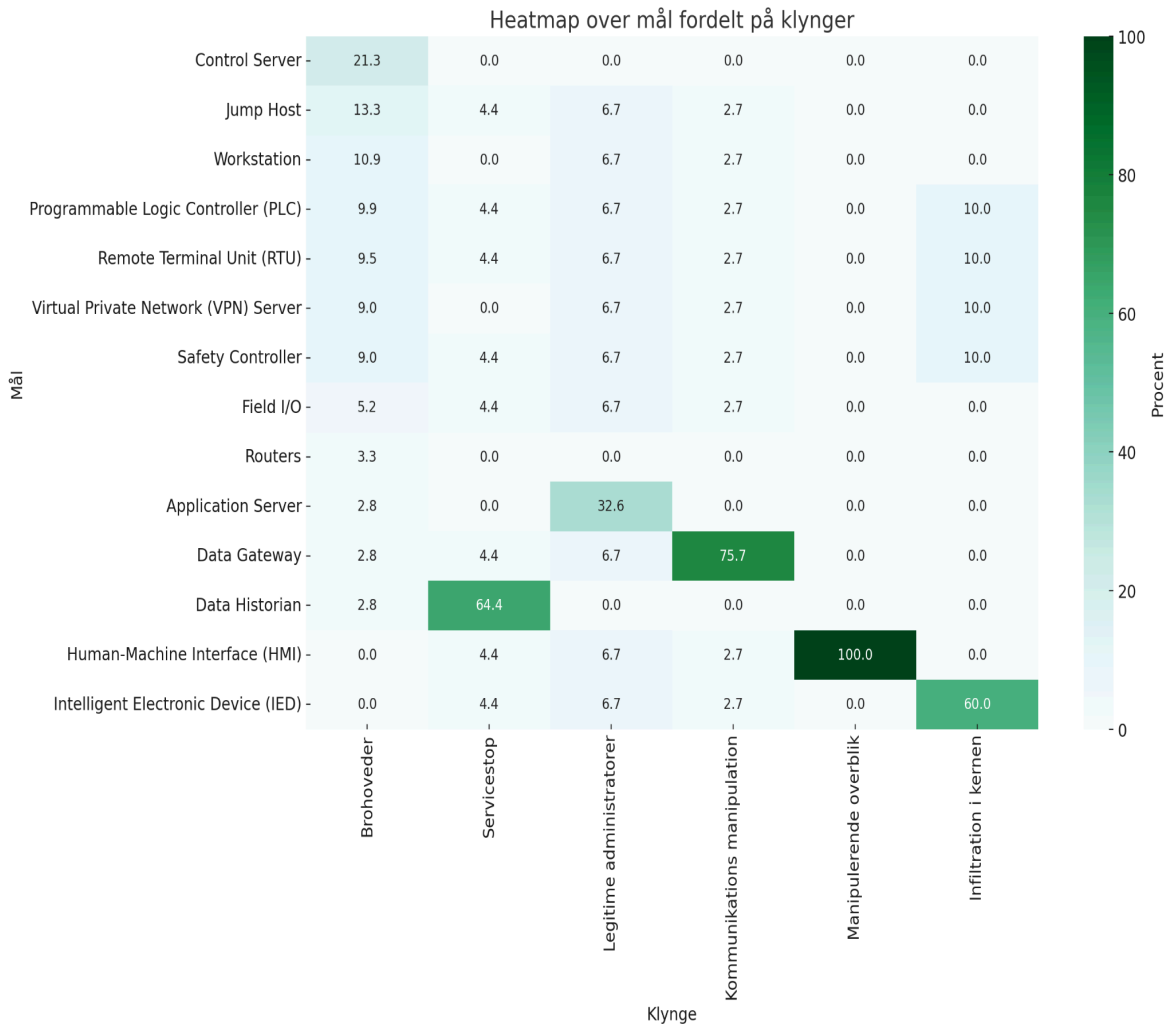
6.1 Inddeling af klynger

Klyngeanalysen har resulteret i seks klynger ud fra variablerne teknikker og mål. Valget om seks klynger er som nævnt tidligere baseret på “elbow-metoden”, hvor kurven har knækket ved seks klynger (se figur 4). De seks klynger udgør tilsammen 460 forskellige observationer. De fordeler sig således, at der i klynge 1 er 211 observationer, i klynge 2 er der 45

observationer, klynge 3 har 89 observationer, klynge 4 har 37 observationer, klynge 5 har 38 observationer og klynge 6 har 40 observationer.

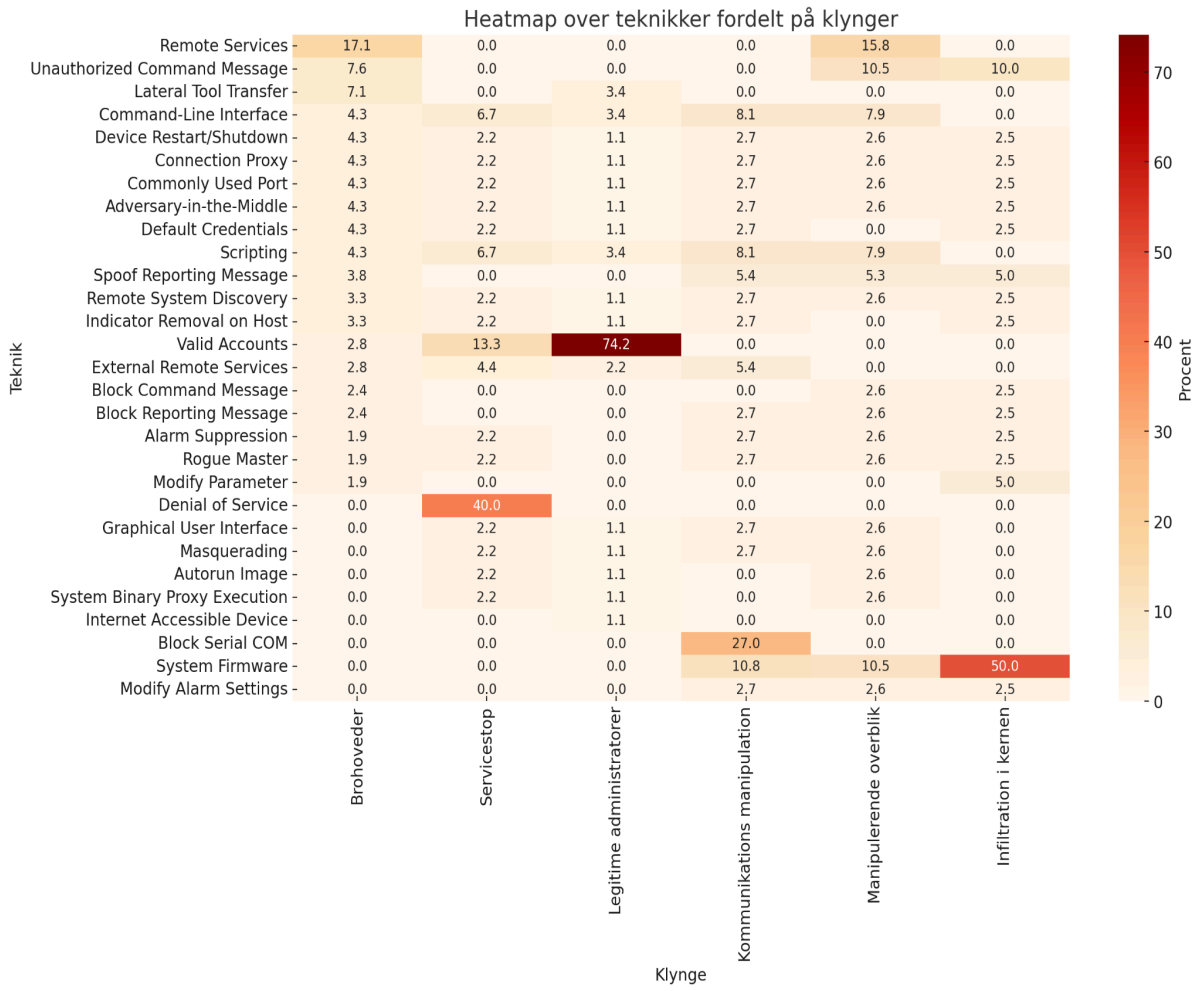
Grundlæggende indeholder klyngeanalysen adskillige variabler i form af forskellige teknikker og mål, hvilket kan gøre uoverskueligt at identificere mønstre. Med mønstre menes forskelle mellem hvordan aktørernes modus operandi har været i kampagnerne, de har foretaget. For den videre del af analysen er der yderligere opstillet kriterier i form af, hvordan cyberangreb adskiller sig. Disse kriterier bygger på variabler der er overrepræsenterede i klyngen, set i forhold til procentfordelingen af hvilke teknikker der er brugt af aktøren, samt hvilke mål de har gået efter internt i klyngen. At fremhæve bestemte værdier betyder også at andre vil blive nedprioriteret, hvilket er en analytisk konsekvens af et komplekst datagrundlag, som er væsentligt at være opmærksom på. Det kan medføre utilsigtet bias i analysen ved at lægge vægt på bestemte variabler (Andersen et al. 2012)

For at visualisere hvad de forskelliger klynger indeholder, vil det herunder blive vist to forskellige heatmaps, der viser fordelingen af teknikker og mål, procentfordelt i klyngerne



Figur 5 - Viser fordeling af mål i klyngerne fordelt på procenttal

Hver søjle repræsenterer de mest hyppigt forekommende mål inden for den enkelte klynge. Visualiseringen tydeliggør, at visse mål såsom Control Server, Data Gateway og Human-Machine Interface (HMI) er særligt centrale i bestemte klynger. Samtidig illustrerer figuren, hvordan cyberangreb mod specifikke mål i det industrielle kontrolsystem varierer markant mellem klyngerne, hvilket peger på forskellige strategiske fokusområder i de observerede angrebsformer.



Figur 6 - Viser fordelingen af teknikker fordelt på procenttal i klyngerne

Hver række repræsenterer de mest anvendte teknikker inden for den pågældende klynge. Figuren synliggør, at visse teknikker som Valid Accounts, System Firmware og Remote Services optræder på tværs af flere klynger, men med varierende intensitet. Samtidig fremhæver visualiseringen, at enkelte klynger domineres af én eller få teknikker, hvilket afspejler forskellige operative tilgange i angrebene.

6.2 Klynge 1 - Brohoveder

6.2.1 Formål

Klynge 1 består af 211 cyberangreb ud af de 460, der er blevet analyseret i dette projekt. Det gør den til den største klynge. Klynge 1, også kaldet Brohoveder, har fået deres navn, idet

aktørerne både har fokus på at have en tilstedeværelse i IT-systemer og det industrielle kontrolsystem. Klyngen repræsenterer en strategisk og teknisk fokuseret form for cyberangreb. Formålet er ikke nødvendigvis at forårsage umiddelbar skade, men snarere at etablere og fastholde adgang til centrale enheder i det industrielle kontrolsystem. Et særligt kendetegn ved denne klynge er, at den rammer enheden Jump Host og derigennem etablerer en tilstedeværelse både i IT-infrastrukturen, samt det industrielle kontrolsystem. Denne adgang giver aktørerne mulighed for at observere, manipulere eller forberede sig på et mere dybtgående cyberangreb på et senere tidspunkt. Det handler med andre ord ikke om at "ødelægge", men om at "komme ind og blive". Cyberangrebene i denne klynge er altså ikke destruktive i første omgang, men udgør et væsentligt sikkerhedsproblem, fordi de lægger fundamentet for potentielt langt mere alvorlige hændelser.

6.2.2 Teknisk analyse

Når vi ser på hvordan cyberangrebene i denne klynge foregår, er det især en teknik, der skiller sig ud: brugen af fjernadgangstjenester, som står for 17,06 % af alle teknikker i klyngen. Derefter følger teknikker, hvor aktøren sender skadelige kommandoer til systemerne (7,58 %) og teknikker, hvor der overføres skadelig software mellem systemer (7,11 %). Fjernadgangstjenester dækker over teknologier som Remote Desktop Protocol (RDP), Secure Shell (SSH) og Server Message Block (SMB). Det er teknologier, der gør det muligt at styre en computer eller en server, selvom man fysisk sidder et helt andet sted. Man kan for eksempel overtage skærmen på en PC, sende filer mellem systemer eller få adgang til netværksdrev (Mitre, 2021c). I industrielle kontrolsystemer bruges disse teknologier også af teknikere og operatører til at vedligeholde og tilgå systemerne på afstand. Problemet er, at hvis uvedkommende aktører får adgang til disse tjenester, kan de bevæge sig fra ét system til et andet. Eksempelvis fra en almindelig kontor-PC ind til selve styringen af et anlæg.

En anden teknik, som fylder i klyngen, er at aktøren sender uautoriserede kommandoer til kontrolsystemet. Det kan betyde, at systemet tvinges til at ændre sin adfærd, for eksempel at en motor bliver stoppet, eller en alarm bliver udløst uden at en operatør har godkendt det (Mitre, 2020d). Derudover ses det, at aktørerne ofte flytter deres skadelige software rundt mellem systemer for at opbygge deres kontrol trin for trin. Det gøres typisk ved hjælp af SMB, som normalt bruges til at dele filer internt i netværket (Mitre, 2020e)

Cyberangrebene i klyngen Brohovederne rammer især de centrale dele af systemet herunder Kontrolservere (21,33 %): Disse fungerer som hjernen i det industrielle system. De styrer, hvad der skal ske i for eksempel maskiner og anlæg, og kommunikerer via protokollen Modbus (Mitre, 2023f). Jump Hosts (13,27 %): Er særlige computere, som kontrollerer adgangen ind til de industrielle systemer. De fungerer som "dørvogtere" mellem virksomhedens normale IT-systemer og det industrielle kontrolsystem (Mitre, 2023g). Til sidst rammer cyberangrebene Arbejdsstationer (10,90 %): Dette er almindelige computere, som teknikere bruger til daglig drift, fejlfinding og vedligehold. (Mitre, 2023h).

6.2.3 Fortolkende analyse

Kigger vi på klyngen Brohoveder i forhold til Walls typologier for cyberkriminalitet, placeres denne klynge inden for både Cyber-Trespass og Cyber-Deception/Theft. Dette fordi aktørerne i denne klynge både indebærer uautoriseret adgang og potentiel udnyttelse af følsomme systemer. Ifølge Walls definition omfatter Cyber-Trespass den uretmæssige indtrængen i computernetværk eller systemer uden ejerens tilladelse (Viano, 2017). Dette er præcist, hvad Brohovederne gør. De etablerer adgang til kritiske enheder som Jump Hosts og Kontrolservere i industrielle kontrolsystemer. Derudover afspejler klyngens mål og teknikker også aspekter af Cyber-Deception/Theft, idet aktøren bruger den opnåede adgang til at manipulere systemer og flytte skadelig software, hvilket kan give adgang til følsomme oplysninger eller operationel kontrol, der har stor værdi. Som Wall fremhæver, er disse to kategorier ofte tæt forbundne, da deception og theft typisk forudsætter trespass (Viano, 2017). I klyngen, Brohovederne, fungerer trespass derfor som en forudsætning for en potentiel senere udnyttelse af systemet og de data, det rummer.

6.3 Klynge 2 - Servicestop

6.3.1 Formål

Klynge 2 består af 45 cyberangreb ud af de 460, der er blevet analyseret i projektet. Klynge 2, også kaldet "Servicestop", adskiller sig fra de andre klynger, da formålet ikke nødvendigvis er at tage kontrol, men snarere at skabe forvirring, usikkerhed og tab af overblik. Hvor andre

aktører forsøger at bevæge sig gennem netværket eller ændre fysiske processer, så handler det her om at slukke for systemets "hukommelse" og dermed blinde operatørerne. På baggrund af denne målsætning klyngen navngivet "Servicestop" fordi det er netop det, aktøren forsøger at opnå: at tage synlighed og forståelse ud af systemet, således man ikke kan drifte processerne i systemet.

6.3.2 Teknisk analyse

40% af cyberangrebene i denne klynge bruger teknikken Denial of Service-angreb. Denial of service-angreb omhandler at overbelaste eller lamme systemer, så de ikke længere virker enten midlertidigt eller permanent (Mitre, 2020i). Sådanne cyberangreb kan udføres på flere måder. Nogle gange sker det ved, at systemet oversvømmes med forespørgsler, så det ikke kan følge med. Andre gange udnytter aktørerne fejl eller svagheder i systemet, der får det til at gå ned. Industrielle kontrolsystemer kan være følsomme, og nogle kan blive lammet bare ved en simpel scanning af netværket.

En anden teknik der er værd at fremhæve i klyngen er, at aktøren ofte har skaffet sig adgang via gyldige brugerkonti (13,33 %). Det kan ske ved hjælp af stjålne adgangskoder eller ved at aktøren allerede har brudt ind tidligere (Mitre, 2020j). Fordelen for aktøren er, at det gør deres aktiviteter meget sværere at opdage, da de bruger samme adgang som legitime brugere.

Det særlige ved klyngen er, at næsten alle cyberangrebene er rettet mod én specifik del af det industrielle kontrolsystem: Data historikeren, som er mål for hele 64,44 % af cyberangrebene. En Data historiker er det system, der opsamler og gemmer historiske data for eksempel hvordan temperaturer, tryk eller strømforbrug har udviklet sig over tid (Mitre, 2023k). Det er et afgørende værktøj for både overvågning og analyse, og uden det bliver det svært for operatører at forstå, hvad der foregår i systemet . Et cyberangreb på denne komponent kan gøre det umuligt at se, om der er problemer i systemet.

6.3.3 Fortolkende analyse

Klyngen "Servicestop" placerer sig mest oplagt inden for Walls typologi Cyber-violence, da angrebene har til hensigt at skade og forstyrre funktionaliteten i industrielle kontrolsystemer.

Ifølge Walls definition dækker Cyber-violence over handlinger, hvor teknologi bruges til at true eller forvolde skade på personer eller institutioner (Viano, 2017) Hvilket her manifesterer sig som Denial of Service-angreb, der lammer essentielle systemer. Når angrebene målrettet slår "systemets hukommelse" ud gennem Data historikeren medfører det ikke kun teknisk dysfunktion, men også usikkerhed for operatørerne, hvilket netop er formålet. Dette udgør en form for indirekte vold mod systemets evne til at fungere og mod dem, der er afhængige af det.
Derudover ses en mindre, men væsentlig, tilknytning til Cyber-deception/theft, i det omfang angriberne anvender gyldige brugerkonti, typisk ved stjålne legitimationsoplysninger. Dette involverer elementer af bedrag, som gør det muligt at udføre angrebene uset og camoufleret som legitime brugere (Viano, 2017).

6.4 Klynge 3 - "Legitime" Administratorer

6.4.1 Formål

Klynge 3 består af 89 cyberangreb ud af de 460, der er blevet analyseret i projektet. Det gør den til den næststørste klynge. Denne klynge, også kaldet "Legitime Administratorer", er præget af en meget diskret og sofistikeret angrebsform. Det, der adskiller denne klynge fra andre, er den stille og skjulte metode. Hvor andre angribere måske forsøger at nedlægge systemer eller blokere funktioner, så handler det her om at glide ubemærket ind og agere som om man var en helt almindelig administrator. På den baggrund navngives klyngen "Legitime Administratorer" – fordi aktøren netop udnytter legitim adgang til at udføre handlinger uden at skabe alarm. De opfører sig som en del af systemet og skjuler deres aktivitet bag almindelig drift.

Et centralt formål med angrebene i klyngen er at opretholde et skjult og stabilt fodfæste i det industrielle kontrolsystem. Aktørerne forsøger ikke blot at få adgang én gang, men at sikre, at denne adgang kan bevares over tid, selv hvis systemet genstartes, loginoplysninger ændres, eller der sker anden form for oprydning eller sikkerhedstiltag.

6.4.2 Teknisk analyse

I 74% af tilfældene bruger aktørerne i denne klynge teknikken kompromitterede, men gyldige, loginoplysninger til at få adgang til systemet. På samme måde som i klynge 2 "Servicestop" logger aktøreren ind som autoriseret bruger via. gyldig loginoplysninger (Mitre, 2020j). Det gør det svært at opdage, fordi intet i sig selv virker mistænkeligt, da der bliver logget ind med rigtige brugernavne og adgangskoder. Adgangen kan som tidligere nævnt være opnået ved stjålne oplysninger gennem phishing eller en insider – altså en person, der allerede arbejder i organisationen og misbruger sine egne rettigheder.

Når man ser på, hvilke dele af det industrielle kontrolsystem der bliver angrebet, er det relativt bredt fordelt. Den mest ramte enhed er Applikationsservere (32,60 %), som typisk kører programmer, der styrer eller understøtter driften (Mitre, 2023l). Når aktørerne rammer applikationsserveren, får de adgang til et centralt kontrolpunkt i systemet, som både giver dem indsigt, påvirkningsmuligheder og en platform for videre infiltration – alt sammen uden nødvendigvis at vække mistanke.

6.4.3 Fortolkende analyse

Denne klynge er præget af, at aktørerne benytter kompromitterede loginoplysninger, hvilket muliggør adgang uden at vække mistanke. Denne form for "usynlig" adgang passer godt til Walls idé om cyber-trespassing som en type kriminalitet, hvor grænseoverskridelsen i sig selv er det centrale. Aktøren bevæger sig ind i et rum, de ikke har retmæssig adgang til, og gør det ofte uden umiddelbart at ændre eller ødelægge noget (Viano, 2017). Det gør ikke angrebet mindre alvorligt – tværtimod – men det betyder, at skaden ligger i selve overtrædelsen og den potentielle kontrol, som aktøren opnår over industrielle kontrolsystemer.

Særligt i en kontekst af industrielle kontrolsystemer, hvor driftsstabilitet og sikkerhed er altafgørende, er denne type cyberangreb bekymrende, fordi den kan pågå over længere tid uden at blive opdaget. Det åbner for både datatyveri, manipulation og senere destruktive handlinger – alt sammen udført fra en position, der ser ud som en del af den almindelige drift. Dermed viser klyngen, hvordan cyber-trespassing i moderne industrielle kontrolsystemer kan antage meget sofistikerede og lavprofilerede former, der kræver avanceret overvågning for at blive identificeret.

6.5 Klynge 4 - Kommunikations Manipulation

6.5.1 Formål

Klynge 4 består af 37 cyberangreb ud af de 460, der er blevet analyseret i projektet. Denne klynge, navngivet “Kommunikations Manipulation”, grundet dennes fokus på kommunikationsvejene i det industrielle kontrolsystem. Klygen skiller sig ud ved, at den handler om at afbryde eller forstyrre selve kommunikationen mellem dele af det industrielle kontrolsystem. Formålet med angrebene i denne klynge er at undergrave systemets evne til at reagere korrekt på farlige eller uønskede situationer. Det sker ikke gennem direkte ødelæggelse, men gennem en systematisk forstyrrelse af de enheder, der skal beskytte drift, sikkerhed og kvalitet i det industrielle kontrolsystem. Ved at manipulere eller afbryde de kommunikationsveje og funktioner, der forbinder målinger, styring og menneskelig indgriben, skaber aktørerne et system, der ikke længere ser, hvad der sker eller reagerer rigtigt på det.

6.5.2 Teknisk analyse

I 27% af tilfældene handler det om at blokere den serielle kommunikation – altså den direkte "snak" mellem to fysiske enheder, som ofte foregår via ledninger og porte, og som bruges til at styre og aflæse kritiske processer(Mitre, 2020m). Når denne kommunikation bliver forstyrret, risikerer systemet at miste overblikket over, hvad der egentlig sker i anlægget.

Yderligere teknikker der bliver brugt i klyngen er, at aktøren forsøger at ændre den grundlæggende software i enhederne i 10,8% af cyberangrebene, Ved at ændre den grundlæggende den grundlæggende software, der styrer enheden på et lavt niveau (Mitre, 2020n). Der ses også teknikker som automatiserede scripts og ændring af kommandolinjer på enkelte enheder i henholdsvis 8,11% af tilfældene for begge teknikker. Automatiserede scripts gør, at aktørerne kan ændre et eller flere systemer. Da automatiserede scripts ikke behøver interaktion fra aktørens side, kan det “selvkøre” og sprede malware på mange systemer (Mitre, 2020p) hvorimod hvis aktøren ændrer kommandolinjer, foregår det på enkelte enheder og kræver interaktion fra aktøren (Mitre, 2020o).

Det hyppigste mål i denne klynge er Data Gateways, som bliver angrebet i 75 % af tilfældene. Data Gateways fungerer som "oversættere" og forbindelser mellem forskellige dele af det industrielle kontrolsystem. De sørger for, at data kan flyde frit mellem måleenheder, styringssystemer og operatørers HMI'er (Mitre, 2023q). Hvis en aktør får adgang til disse gateways, kan de afbryde kommunikationen, fjerne vigtige data, eller indsætte falske oplysninger, der får systemet til at tro, at alt er i orden, når det ikke er. Det vil i sidste ende kunne skabe uhensigstmæssige situationer hvor systemet kører og er i drift, men at det opererer "forkert" idet inputs til systemet er forkerte. Dette er ikke et direkte destruktivt angreb på systemet, men nærmere på hvad systemet understøtter.

6.5.3 Fortolkende analyse

Ser man denne klynge ud fra Walls typologier er Cyber-violence passende her. Wall beskriver Cyber-violence som brugen af informationsteknologi til at true eller skade individer eller samfund. Det dækker ikke kun over direkte vold eller chikane, men også over mere strukturelle og infrastrukturelle former for skade (Viano, 2017). I denne klynge ses netop et sådant mønster. Cyberangrebene forårsager ikke nødvendigvis øjeblikkelig ødelæggelse, men de lammer systemets evne til at opdage, advare og handle i kritiske situationer. Når for eksempel en Data gateway manipuleres til at sende forkerte oplysninger, eller når en alarmfunktion bevidst saboteres, kan det medføre, at anlægget opererer i en farlig tilstand uden operatørens viden. Dette udgør en indirekte, men potentielt livstruende form for cyber-violence, især i tilfælde hvor den industrielle proces understøtter den kritiske infrastruktur.

6.6 Klynge 5 - Manipulerende overblik

6.6.1 Formål

Klynge 5 består af 38 cyberangreb ud af de 460, der er blevet analyseret i projektet. Klyngen er navngivet "Manipulerende overblik", grundet aktørens fokus på ikke nødvendigvis fysisk ødelæggelse, men snarere at narre operatøren, ved at ændre brugergrænseflader og derigennem skjule den egentlige systemtilstand. Ligeledes som klynge 3, "Legitime

Administratorer", er det samlede billede i denne klynge ikke fysisk ødelæggelse, men om at ændre operatørens opfattelse af virkeligheden. Det er altså ikke maskinerne, der angribes direkte, men menneskets øjne og forståelse af, hvad maskinerne gør. Ved at forvride informationer og sende falske signaler, kan aktøren skabe usikkerhed, skjule sabotage eller få operatøren til selv at træffe forkerte beslutninger.

6.6.2 Teknisk analyse

Cyberangrebene er 100% målrettet mod én bestemt komponent i det industrielle kontrolsystem, nemlig HMI'er. Det er de skærme og brugerflader som operatørerne bruger til at overvåge og styre processer i anlægget. Hvis en HMI bliver manipuleret, kan det få operatøren til at se noget andet end det der faktisk sker, og det gør dem til et særdeles sårbart mål (Mitre, 2023r).

Klyngen er teknisk præget af tre centrale teknikker, herunder Fjernadgang (15,79 %) – hvor angriberen opnår adgang til HMI'en gennem teknologier som tidligere nævnte RDP's eller SSH's, som normalt bruges til at arbejde på en computer fra afstand (Mitre, 2021c). Denne teknik er også den meste brugte i klynge 1 "Brohovederne", her var teknikken dog rettet mod Jump Hosten. Lige såvel som klynge 4 og 6, gør aktørerne i denne klynge også brug af Firmwaremanipulation (10,53 %) – Her ændrer aktøren den grundlæggende software, der styrer enheden på et lavt niveau (Mitre, 2020n). Yderligere bruger de også uautoriserede kommandoer (10,53 %) – hvor HMI'en bruges til at sende skadelige beskeder til kontrolsystemet, uden at det nødvendigvis opdages (Mitre, 2020d).

Kombinationen af disse teknikker udgør et cyberangreb, hvor aktøren både har adgang til systemet og den tekniske viden til at manipulere det på et dybt og avanceret niveau. Det kan betyde, at operatøren kigger på en skærm, der viser "alt er normalt", mens systemet i virkeligheden er kompromitteret eller allerede reagerer på skjulte kommandoer. Når firmware bliver ændret, kan det ske på en måde, som ikke umiddelbart kan ses eller opdages, heller ikke af IT-systemer, der ellers overvåger sikkerheden. Det gør cyberangrebet farligt, fordi det kan blive siddende længe og manipulere systemet over tid uden at blive opdaget.

6.6.3 Fortolkende analyse

Klyngen Manipulerede overblik kan med udgangspunkt i Walls typologi over cyberkriminalitet primært placeres under Cyber-deception/theft, med væsentlige elementer af Cyber-trespass.

Først og fremmest er klyngens fokus, at cyberangrebene er målrettet HMI'er, de visuelle brugerflader, hvor operatører overvåger og styrer de industrielle processer. Formålet med disse angreb er ikke blot at få adgang, men at manipulere den information, operatøren ser og handler ud fra, hvilket gør klyngen til et klart eksempel på Cyber-deception. Wall definerer denne typologi som brugen af informations- og kommunikationsteknologi til at bedrage og snyde. Enten for at tilegne sig noget af værdi eller for at narre ofre til at foretage bestemte handlinger (Viano, 2017). I dette tilfælde er det ikke den klassiske økonomiske gevinst, der søges, men snarere operationel manipulation og fordrejning af virkeligheden, som kan føre til både forkert beslutningstagning og utilsigtede handlinger i driften.

Samtidig er der tydelige træk af Cyber-trespass, idet aktøren opnår adgang til systemet uden tilladelse, ofte gennem fjernadgangstjenester som RDP og SSH. Ifølge Wall indebærer trespass at krydse digitale grænser uden tilladelse, og i denne klynge sker det netop for at få adgang til HMI'en og manipulere den indefra (Viano, 2017). Adgangen er ikke blot et middel til at komme ind, men en nødvendig forudsætning for at udføre den mere subtile manipulation, der følger.

6.7 Klynge 6 - Infiltration i kernen

6.7.1 Formål

Klynge 6 består af 40 cyberangreb ud af de 460, der er blevet analyseret i projektet. Denne klynge, er navngivet "Infiltration i kernen", på grund af klyngens fokus på manipulation af centrale styringsenheder, dens tekniske dybde og dens evne til at operere skjult og langvarigt. Dette fordi angrebet sker dybt inde i de komponenter, der styrer hele systemet, og kontrollerer processerne i det skjulte.

Klyngen skiller sig ud ved at handle om manipulation af selve kernen i de enheder, der styrer industrielle processer. Formålet med angrebene i klyngen er at forhindre systemets sikkerhedsfunktioner i at træde i kraft ved farlige eller uforudsete hændelser. Dette gøres gennem avancerede teknikker, hvor aktøren ændrer eller manipulerer selve den grundlæggende software, altså firmware i centrale styringsenheder som IEDs, PLC'er og safety controllers. Ved at foretage indgreb dybt i systemets logik og kontrolniveau, undermineres de mekanismer, der normalt skal sikre, at systemet reagerer korrekt på fejltilstande, ulykker eller farlige scenarier.

6.7.2 Teknisk analyse

Halvdelen (50 %) af de angreb, der er analyseret i denne klynge, går direkte efter den grundlæggende software, som styrer hvordan enhederne fungerer også kaldet firmware. Det er den software, der ligger allerlængst nede i systemet og styrer kommunikationen mellem hardwaren og styresystemet. Når den først er ændret, kan aktøren få næsten usynlig og langvarig kontrol og cyberangrebet kan være meget svært at opdage eller fjerne Mitre, 2020n).

Yderligere indeholder klyngen teknikkerne Uautoriserede kommandoer (10%). Her sendes der kommandoer til systemet, som kan få det til at reagere skadeligt eller utilsigtet. Herigennem sendes falske rapporter tilbage til operatøren, så systemet ser ud til at køre normalt, selv når det ikke gør det. Indstillinger ændres inde i systemet, så det reagerer anderledes end forventet, uden at der nødvendigvis er synlige tegn på ændringen. (Mitre, 2020d) Denne form for cyberangreb går ikke bare ud på at få adgang til netværket eller overtage PC'er. Her handler det om at komme helt ind i selve styringsenheden, ændre på dens grundfunktioner og forblive skjult.

De enheder, der bliver ramt, er i høj grad smarte styringsenheder, kaldet Intelligent Electronic Devices (IEDs) – som står for 60 % af målene i denne klynge. Disse enheder bruges til at styre og overvåge strømforsyning og andre vigtige funktioner i et industrielt kontrolsystem (Mitre, 2023s). Hvis en aktør overtager en IED, kan de ændre hvordan strømmen fordeles, hvad der måles, og hvad der rapporteres. Dette kan få alvorlige konsekvenser for både drift og sikkerhed. Resten af cyberangrebene bliver målrettet i 10% af tilfældene. Dette er PLC'er

som styrer lokale maskinprocesser (Mitre, 2023t), RTU'er der indsamler data og styrer systemer på afstand (Mitre, 2023u), Safety Controllers som beskytter både mennesker og maskiner Mitre, 2023v) og VPN-servere som forbinder systemet med omverdenen (Mitre, 2023x)

Det særlige ved denne klynge er, at den ikke handler om at komme ind udefra via netværket, men om at ændre, hvad enhederne rent faktisk gør helt nede i deres inderste. Det er den eneste klynge, hvor firmware-angreb er den mest brugte teknik, og hvor hele fokus ligger på at overtage og manipulere de styrende enheder selv, i stedet for at bevæge sig rundt i netværket. Denne type angreb er svær at opdage og kan sidde "sovende" i lang tid, indtil de aktiveres. De kan også bruges til at manipulere målinger og handlinger i anlægget, så det enten reagerer forkert eller slet ikke reagerer, alt imens operatøren tror alt er normalt.

6.7.3 Fortolkende analyse

Ud fra Walls fire typologier over cyberkriminalitet kan denne klynge primært placeres under kategorien cyber-deception/theft, med tydelige forbindelser til cyber-trespass, og også cyber-violence. Ifølge Wall omfatter cyber-deception/theft former for digital kriminalitet, hvor teknologier anvendes til at narre, manipulere eller bedrage med henblik på at tilegne sig data, systemadgang eller ressourcer, typisk uden umiddelbar fysisk skade (Viano, 2017). Cyber-trespass dækker derimod over uautoriseret adgang til systemer eller netværk, som i sig selv kan være skadevoldende eller fungere som forudsætning for yderligere skadelige handlinger (Viano, 2017).

Klyngen bør først og fremmest forstås som et eksempel på cyber-deception/theft. Dette begrundes med klyngens primære karakteristika, som omfatter avanceret manipulation af systemfunktionalitet og forvrængning af operatørers perception af den faktiske systemtilstand. Ved at ændre eller maskere systemdata opstår en form for digital bedrag, hvor angriberen opnår strategisk fordel gennem vildledning snarere end direkte ødelæggelse.

Samtidig forudsætter denne type angreb som regel en forudgående eller parallel cyber-trespass-handling, da adgang til systemet er en teknisk nødvendighed for at kunne gennemføre manipulationen. I visse tilfælde, særligt hvor manipulationen fører til driftsforstyrrelser eller sikkerhedsbrud med samfundsmæssig eller menneskelig konsekvens,

kan angrebene desuden opnå karakter af cyber-violence, i tråd med Walls bredere forståelse af vold i cyberspace som strukturel og infrastrukturel skade.

6.8 Opsamling af klyngeanalysens hovedfund

Nedenstående afsnit vil være en kort opsummerende afsnit på klyngeanalysens hovedfund. Analysen har identificeret seks overordnede klynger af cyberangreb mod industrielle kontrolsystemer, der hver er karakteriseret ved særlige teknikker og mål. Selvom visse teknikker og mål går på tværs af flere klynger, viser resultaterne, at hver klyngerne også adskiller sig fra hinanden. Det følgende afsnit sammenfatter disse forskelle og belyser, hvordan de forskellige klynger repræsenterer varierende typer af cyberangreb.

Visse teknikker og mål går på tværs i flere af klyngerne, dog viser analysen at hver klynge også har særtræk der gør, at de adskiller sig fra hinanden. Klynge 1, Brohovederne, er karakteriseret ved anvendelsen af et fokus på etablering af fjernadgange og bevægelse mellem IT-infrastrukturen og det industrielle kontrolsystem. Hertil kommer Klynge 2, Servicestop, som er domineret af af teknikken Denial of Service, og dermed er et klart fokus i denne klynge er, at forstyrre data og derigennem den industrielle proces. Hertil kommer klynge 3, "Legitime" administratorer der adskiller sig ved at være meget afhængig af, at bruge legitime adgange for den vedvarende kontrol. I modsætning hertil fokuserer klynge 4, Kommunikations Manipulation, på lavniveauelementer med Data Gateway som primært mål, hvilket antyder manipulation af kommunikation på maskinelt niveau. klynge 5, Manipulerende overblik, skiller sig ud ved at målrette sig mod den menneskelige grænseflade, med 100 % fokus på HMI'er, og brug af teknikker, der kombinerer fysisk og logisk manipulation. Endelig er klynge 6, Infiltrationen i kernen, kendetegnet ved sin tekniske dybde og fokus på ændringer af lavniveuaet som ligeledes blev brugt i klynge 5 og 6, samt et bredt spænd af mål i det industrielle kontrolsystem.

Disse analytiske fund er blevet tolket ud fra Walls typologier om cyberkriminalitet og vil blive diskuteret yderligere i følgende afsnit.

7.0 Diskussion

Formålet med dette diskussionsafsnit er at give læseren bedre grundlag for at vurdere undersøgelsens gyldighed (Andersen et al, 2012). Dette afsnit vil diskutere Walls teoretiske perspektiver og hvordan klyngerne er fortolket ud fra dette. Yderligere vil valg af data og metode blive gennemgået, samt hvordan disse valg kan have implikationer for undersøgelsens resultater, og hvor retvisende resultaterne er.

7.1 Teoretiske perspektiver på klyngernes adfærd

Walls fire typologier over cyberkriminalitet herunder Cyber-trespass, Cyber-deception/ theft, Cyber-pornography/obscenity og Cyber-violence udgør en af de mest anvendte typologier inden for cyberkriminalitet (Viano, 2017). I analysen af dette projekts klynger har det vist sig at klyngerne adskiller når man kigger på brugen af teknikker og ramte måleenheder. Klyngerne i analysen kan placeres i Walls typologier, dog på et overordnet niveau. Klyngerne viser, at Walls kategorier sjældent optræder isoleret, men i praksis ofte overlapper.

Eksempelvis illustrerer klynge 1, Brohoveder, tydeligt en bevægelse fra cyber-trespass, hvor aktøren opnår uautoriseret adgang til cyber-deception/theft, idet adgangen muliggør udnyttelse af systemer eller tyveri af data. En lignende dobbelttydighed gør sig gældende i klynge 5, “Manipulerede overblik”, og klynge 6, “Infiltration i kernen”, hvor både adgang, manipulation og potentiel systemskade indgår. Dette antyder, at moderne cyberangreb særligt rettet mod industrielle kontrolsystemer ofte er hybride i deres karakter, og at det analytisk kan være mere frugtbart at betragte Walls typologi som et spektrum snarere end som adskilte kategorier.

Klynge 2, “Servicestop”, placerer sig mest oplagt under cyber-violence, idet angrebene har til hensigt at forstyrre eller lamme funktionalitet i industrielle kontrol systemer. En udvidelse, af dette begreb ville være særligt relevant i konteksten af industrielle kontrolsystemer, hvor konsekvenserne af angreb kan manifestere sig som samfundsmæssige risici og driftsafbrydelser. På samme måde illustrerer klynge 4, “(Man-in-the-middle-angreb)”, den form for indirekte og systemisk skade, som Walls begreb om cyber-violence ikke nødvendigvis rummer (Viano, 2017).

Endvidere rummer analysen også en teoretisk gråzone i klynge 3, "Legitime administratorer", hvor adgangen ikke nødvendigvis er teknisk uautoriseret, men sker på baggrund af tildelt og måske misbrugt legitimitet. Her udfordres grænsen for cyber-trespass og illustrerer, hvordan sociale og organisatoriske faktorer kan komplicere den analytiske forståelse af adgang og ansvar.

Samlet set bekræfter klyngeanalysen Walls typologis anvendelighed som strukturerende ramme for at forstå forskellige typer cyberangreb. Samtidig peger analysen på behovet for teoretisk fleksibilitet, da mange angreb i praksis kombinerer elementer af adgang, manipulation og skade, og dermed undlader entydig kategorisering. Dette understreger den hybride karakter af moderne cybertrusler mod industrielle kontrolsystemer og nødvendigheden af at fortolke Walls model dynamisk.

De moderne cyberangreb som analysen i dette projekt afdækker, er præget af høj teknisk kompleksitet, langsigtede strategier og aktører med specifikke mål, som for eksempel at lamme systemer, manipulere sensordata eller forstyrre operatørens beslutningsgrundlag. Disse aspekter overskrider Walls rammer, som ikke differentierer mellem for eksempel et cyberangreb på firmware eller en manipulation af kontrolenheder. Walls typologier er i sin natur ikke designet til at indfange teknologisk dybde, systemisk kontekst eller faser i et angreb, og den forudsætter implicit, at cyberkriminalitet kan forstås gennem relativt faste intentionelle og adfærdsmæssige kategorier (Viano, 2017).

Men i praksis overlapper cyberangreb ofte hinanden, skifter form over tid og udfolder sig i en sekvens af taktiske valg, hvor cyber-trespass blot er første skridt i en langt mere kompleks angrebsstrategi. Derfor bliver Walls typologi analytisk utilstrækkelig som ramme for forståelse, når cyberangreb ikke blot handler om adgang eller tyveri, men om at infiltrere, styre eller ændre hele systemets funktion. Hvis man vil besvare problemformuleringen – hvordan cyberangreb mod industrielle kontrolsystemer adskiller sig fra hinanden – er det derfor nødvendigt at supplere de overordnede forståelsesrammer med en dybere teknisk analyse. Det betyder, at man må undersøge de anvendte teknikker for eksempel firmwaremanipulation eller fjernadgang. Samt de målrettede systemkomponenter HMI, IEDs, gateways med mere, og den hensigt, aktøren forfølger – for eksempel om det handler om adgang, skjult kontrol, manipulation af af det operatøren ser, eller forberedelse til fremtidig skade. Kun ved at analysere angrebene på dette niveau af teknisk granularitet, er det muligt at forstå deres forskellighed i praksis.

Med andre ord kan Walls typologier fungere som indledende analytiske rammer, men en dybdegående undersøgelse af teknikker, mål og systemeffekter er afgørende for at opnå den nuancerede forståelse, som opgavens problemformulering kræver.

7.2 Valg af data og metode

Valget af sekundære data fra Mitre Attack har givet projektet en solid og struktureret tilgang til at analysere cyberangreb mod industrielle kontrolsystemer. Som tidligere redegjort for giver Mitre Attack adgang til et opdateret datasæt, som bygger på empirisk dokumenterede kampagner (Alexander et al. 2020). Det har muliggjort en systematisk klyngeanalyse baseret på observerbare teknikker og mål. Ikke desto mindre medfører brugen af sekundær data en række metodiske og analytiske begrænsninger, der har betydning for både fortolkning og generaliserbarhed.

En væsentlig begrænsning ved det anvendte datasæt er, at det udelukkende fokuserer på kampagner, næsten udelukkende fra APT'er. Som tidligere redegjort for er disse aktører typisk statsstøttede eller særligt ressourcestærke grupper med langsigtede, strategiske mål, hvilket betyder, at datasættet i høj grad repræsenterer relativt sofistikerede angreb (CFCS, 2024b). Dermed går data om økonomisk motiverede aktører – såsom cyberkriminelle grupper, ransomware-operatører eller aktivistiske grupper i vid udstrækning tabt. I stedet begrænser det analysen til at identificere variationer inden for én aktørtype, hvilket giver dybde i forståelsen af APT-kampagner, men udelukker vigtige forskelle i aktørernes modus operandi på tværs af trusselbilledet som kunne være til stede i et mere mangfoldigt datasæt. Dette har konsekvenser for projektets generaliserbarhed og understreger behovet for fremtidige studier, der også inddrager bredere trusselsaktørkategorier.

I relation til problemformuleringen betyder det, at projektets svar på, hvordan cyberangreb adskiller sig fra hinanden, primært gælder forskelle internt blandt APT'er, og ikke nødvendigvis bredt i hele trusselslandskabet.

Derudover skal det anerkendes, at de teknikkategorier, som Mitre Attack anvender, i visse tilfælde er relativt brede. Selvom kategorierne tilbyder en veldefineret taksonomi, kan en teknik som for eksempel "Fjernadgang" eller "Brugen legitime konti" dække over meget forskellige tekniske implementeringer og angrebsscenarier. Uden en dybere nedbrydning

risikerer man at gruppere angreb sammen, som i praksis opererer med forskellige formål, tekniske niveauer og grader af konsekvens. Dette stiller krav til forskeren om at være kritisk i tolkningen af, hvad en given teknik faktisk indebærer (Singer & Friedmann, 2014)

Et metodisk valg der taget i processen var fravalget af variablen "Taktikker", for at have et udelukkende fokus på teknikker og mål. Dette har gjort at analysen er blevet orienteret mod den operationelle del af cyberangrebene frem for den overordnede taktiske del. I analysen er der givet et bud på hvad formålet har været med sammensætningen af teknikker og mål. Dette har dog ikke taget udgangspunkt i de klassiske taktikker som Mitre tilbyder. Mitre Attack organiserer deres teknikker under overordnet taktikker således det er muligt at differentiere i hvilken fase af et angreb en given teknik bruges. Taktikker forstås altså som led i et angreb, som eksempelvis kan være "indledende adgang", "lateral bevægelse" eller "Kollektion" (Mitre, n.d.y). Dette afspejler sig i klyngeanalysen ved, at nogle klynger indeholder teknikker, der udelukkende ses brugt i en fase af et angreb. Dette gælder for eksempel klynge 3 "Legitime administratorer" som gør brug legitime brugerkonti, der hører under taktikken Persistence (fodfæste) og Lateral movement (Lateral bevægelse) (Mitre, 2020j). Disse overordnede taktikker siger ikke noget om cyberangrebenes overordnede formål, i forhold til om det er eksfiltrering af data, kryptering af data eller sabotage. Det siger noget om en fase aktøren er i, gennem hele cyberkampagnen.

Problemformuleringen fordrer ikke at skulle adskille cyberangrebenes overordnede formål, men det er et perspektiv der er relevant at undersøge. Cyberangreb har forskellige formål når de opererer inden for industrielle kontrolsystemer, men dataen på angrebene er dog sparsomme, og det er en nødvendighed ved brug af kvantitative undersøgelser, at der er "nok" data at analysere.

En vigtig konsekvens af dette er, at analysens fortolkningsramme ændres: Hvor en traditionel Mitre-baseret analyse med både taktikker og teknikker kunne fremhæve, hvilke mål eller intentioner der ligger bag visse cyberangrebangreb, fokuserer denne klyngeanalyse snarere på, hvordan cyberangreb udfolder sig teknisk. Dette kan give dyb indsigt i angrebets progression og i de specifikke tekniske afhængigheder, som kendetegner forskellige angrebstyper.

Trods disse begrænsninger viser analysen, at det er muligt at identificere meningsfulde og adskilte tekniske angrebsprofiler alene på baggrund af teknikker og mål. Det peger på, at der

eksisterer underliggende strukturelle forskelle mellem forskellige typer af cyberangreb mod industrielle kontrolsystemer, som kan afdækkes uden nødvendigvis at inddrage taktikkerne eksplicit.

Samtidig lægger analysens resultater op til videre forskning, hvor teknikkerne i højere grad kombineres med deres tilhørende taktikker for at opnå en mere nuanceret forståelse af både angrebets struktur og formål. En fremtidig tilgang kunne være at inddrage hele Mitre Attack-rammeværket i en flerlaget analyse, hvor klynger ikke blot defineres ud fra teknisk sammenhæng, men også ud fra taktisk og strategisk betydning. Det ville give mulighed for en mere helhedsorienteret karakterisering af trusselsaktørers modus operandi, hvilket kan være særligt værdifuldt i forsvar og beskyttelse af kritisk infrastruktur.

8.0 Konklusion

Dette speciale har haft til formål at udvide forståelsen for truslerne i cyber-domenet, nærmere bestemt cyberangreb mod industrielle kontrolsystemer. Den valgte problemformulering har betydet et fokus på, hvordan tidligere sete cyberangreb udført mod industrielle kontrolsystemer, adskiller sig fra hinanden med afsæt i, hvilke teknikker aktørerne bruger, og hvilke mål i systemet de angriber. Der har dertil været et fokus på at sige noget overordnet omkring formålene med cyberangrebene med afsæt i kombinationen af teknikker og mål.

Til specialet er der brugt klyngeanalyse som metodisk værktøj, og der er taget en eksplorativ og induktiv tilgang som metodisk. Klyngeanalysen har vist som værende en nyttig metode til at identificere mønstre i cyberangrebene som dataen tilbyder, om end der også truffet subjektive valg. Dataen, der ligger til grund for analysen, har desuden skabt udfordringer, der omhandler dens sekundære karakter. Beskrivelsen af teknikkerne brugt i indeværende speciale kan forstås som værende overordnede, og det anerkendes at de kan dække over flere underliggende teknikker, eller forskellige måder at bruge dem på. En yderligere granulering af hvordan disse teknikker har været brugt, ville højne forståelsen cyberangrebene adskiller sig fra hinanden. Yderligere er dataens teknikker inddelt i overordnede taktikker, som skal forstås som værende en fase af et cyberangreb. Med dette for øje udspringer den analytiske udfordring, der handler om at sige noget overordnet omkring cyberangrebene. Den sidste udfordring har været begrænsninger i forhold til de aktører der indgår i datasættet. Dataen

afgrænser sig til at indeholde kendte cyberkampagner udført hovedsageligt af APT'er. Dette afgrænser også analysens resultater til at kun at sige noget om disse aktører, og det konkluderes derfor, at undersøgelsen ikke kan udvides i et bredere spektrum i forhold til hele trusselslandskabet i cyber-domænet.

Med afsæt i hvilke teknikker aktørerne bruger og de mål de rammer i industrielle kontrolsystemer, kan cyberangreb mod industrielle kontrolsystemer siges at adskille sig fra hinanden. Der er grundlag for at pege på, at cyberangrebene kan inddeles i seks forskellige meningsfyldte klynger. Den første klynge, som yderligere adskiller sig ved at være en del større end de resterende fem, har fokus på at have fodfæste både i it-infrastrukturen og det industrielle kontrolsystem, og bevæge sig mellem disse to lag. Den anden klynge har et fokus på at være forstyrrende, eller ødelæggende i forhold til de processer som det industrielle kontrolsystem understøtter. Den tredje klynge har et fokus på bevægelse i systemerne gennem kendt konti, og derigennem holde sig skjult for detektion. Den fjerde klynge har fokus på at opsnappe kommunikationen mellem enheder i det industrielle kontrolsystem, den femte klynge har fokus på at være forstyrrende gennem brugerænsefladerne til det industrielle kontrolsystem, og til sidst har den sjette klynge et fokus på at infiltrerer og forstyrre sikkerheden i kontrolsystemet gennem enkelte enheder i systemets indre. Set ud fra et kriminologisk perspektiv på cyberkriminalitet, har den indeværende undersøgelse brugt Walls typologier for cyberkriminalitet som fortolkende perspektiv. Her adskiller klyngerne sig ved at have fokus på tre typologier, nemlig cyber-deception/theft, cyber-trespass og cyber-violence. Omend flere af klyngerne kan argumenteres for at bruge cyber-trespass da det er en nødvendighed for at udføre cyberangrebene, altså at de har adgang til systemerne eller enhederne. Yderligere kan det her argumenteres at det fortolkende perspektiv fra Wall synes at have sine begrænsninger i forhold til at skulle skildre klyngernes cyberangreb. Flere af typologierne overlapper hinanden på tværs af klyngerne, og det må derfor konkluderes at, granulaitet og teknisk forståelse er en analytisk nødvendighed, for meningsfuldt at kunne adskille cyberangreb mod industrielle kontrolsystemer.

Analytiske fund vurderes at kunne bidrage til en opdateret forståelse af hvordan cyberangreb udføres mod industrielle kontrolsystemer. Dette skal ses som værende i et præventivt i et øjemed med henblik på forebyggende arbejde. Med forebyggende arbejde menes der i dette hensende produktudviklere til industrielle komponenter og ejere af de industrielle processer

der med fordel kan drage nytte af studier som dette, til en bedre forståelse af trusselslandskabet i et hastigt omskiftelig cyber-domæne.

9.0 Litteraturliste

Alexander, O., Belisle, M., & Steele, J. (2020, March). *MITRE ATT&CK® for industrial control systems: Design and philosophy*. The MITRE Corporation. https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf

Andersen, L. B., Binderkrantz, A. S., & Hansen, K. M. (2012). Forskningsdesign. I L. B. Andersen, K. M. Hansen, & R. Klemmensen (Red.), *Metoder i statskundskab* (2. udg., s. 66–95). Hans Reitzels Forlag.

Andersen, L. B., Hansen, K. M., & Klemmensen, R. (2012). Metoder i statskundskab. I L. B. Andersen, K. M. Hansen, & R. Klemmensen (Red.), *Metoder i statskundskab* (2. udg., s. 439–454). Hans Reitzels Forlag.

Botchkovar, E., Cui, K., Antonaccio, O., & Perkins, R. (2025, September). The organized activities of ransomware groups: A social network approach. *Technology in Society*, *73*, Article 102873. https://doi.org/10.1016/j.techsoc.2025.102873

Center for Cybersikkerhed. (2024a, 4. juni). *Center for Cybersikkerhed hæver trusselsniveauet for destruktive cyberangreb*. https://www.cfcs.dk/da/nyheder/2024/center-for-cybersikkerhed-haver-trusselsniveauet-for-destruktive-cyberangreb/

Center for Cybersikkerhed. (2024b, 12. november). *Center for Cybersikkerhed: Ordforklaringer*. https://www.cfcs.dk/da/cybertruslen/ordforklaringer/

Center for Cybersikkerhed. (2024c, 20. september). *Cybertruslen mod Danmark*. https://www.cfcs.dk/da/nyheder/2024/cybertruslen-mod-danmark-2024/

Center for Cybersikkerhed. (2024d, juni). *Et wiper-angrebs anatomi: Hvordan wipere fungerer, og hvordan du forsvarer dig mod dem*. https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/anatomien-af-et-wiperangreb.pdf

Che Mat, N. I., Jamil, N., Yusoff, Y., & Mat Kiah, M. L. (2023, September 22). A systematic literature review on advanced persistent threat behaviors and its detection strategy. *Journal of Cybersecurity*. Oxford University Press. https://doi.org/10.1093/cybsec/tyad023

Clark, T., Foster, L., Sloan, L., & Bryman, A. (2021). *Bryman's social research methods* (6. udg.). Oxford University Press.

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2021, April 15). Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture. *The British Journal of Criminology*. https://doi.org/10.1093/bjc/azab026

Council of Europe. (2001, November 23). *Convention on Cybercrime* [ETS No. 185]. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Det Danske Sprog- og Litteraturselskab. (n.d.). *Adskille*. Den Danske Ordbog. https://ordnet.dk/ddo/ordbog?query=adskille
DPS Telecom. (n.d.). *Understanding Modbus protocol: RTU vs TCP vs ASCII*. https://www.dpstele.com/modbus/index.php

European Commission. (2022). *Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), COM/2022/454 final*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454

European Union Agency for Cybersecurity. (2024, September). *ENISA threat landscape 2024*. https://doi.org/10.2824/0710888

European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union* (NIS 2 Directive). *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32022L2555

Halkidi, M., Batistakis, Y., & Vazirgiannis, M. (2001). On clustering validation techniques. *Journal of Intelligent Information Systems*, *17*(2–3), 107–145. Kluwer Academic Publishers.

Holt, T. J. (2022, September 21). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*. Elsevier. https://doi.org/10.1016/j.chb.2022.107493

İmamoğlu, M. B. (2025). *Cyber infrastructure guide: IT/OT integration*. DergiPark Akademik. https://doi.org/10.25287/ohuiibf.1558269

Lusthaus, J. (2012, May 11). Trust in the world of cybercrime. *Global Crime*, *13*(2), 71–94. https://doi.org/10.1080/17440572.2012.674183

Maynard, P., McLaughlin, K., & Sezer, S. (2020, October 14). Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyaa020

MITRE. (n.d.-a). *MITRE Corporation*. https://www.mitre.org/

MITRE. (n.d.-b). *Campaigns*. https://attack.mitre.org/campaigns/

MITRE. (2021c). *Techniques: T0886 – Remote Services*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0886/

MITRE. (2020d). *Techniques: T0855 – Unauthorized Command Message*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0855/

MITRE. (2020e). *Techniques: T0867 – Lateral Tool Transfer*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0867/

MITRE. (2023f). *ATT&CK asset: A0007*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0007/

MITRE. (2023g). *ATT&CK asset: A0012*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0012/

MITRE. (2023h). *ATT&CK asset: A0001*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0001/

MITRE. (2020i). *Techniques: T0814 – Denial of service*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0814/

MITRE. (2020j). *Techniques: T0859 – Valid accounts*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0859/

MITRE. (2020k). *ATT&CK asset: A0006*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0006/

MITRE. (2020l). *ATT&CK asset: A0008*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0008/

MITRE. (2020m). *Techniques: T0805 – Block serial COM*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0805/

MITRE. (2020n). *Techniques: T0857 – System firmware*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0857/

MITRE. (2020o). *Techniques: T0807 – Command line interface*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0807/

MITRE. (2020p). *Techniques: T0853 – Scripting*. MITRE ATT&CK®. https://attack.mitre.org/techniques/T0853/

MITRE. (2023q). *ATT&CK asset: A0009*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0009/

MITRE. (2023r). *ATT&CK asset: A0002*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0002/

MITRE. (2023s). *ATT&CK asset: A0005*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0005/

MITRE. (2023t). *ATT&CK asset: A0003*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0003/

MITRE. (2023u). *ATT&CK asset: A0004*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0004/

MITRE. (2023v). *ATT&CK asset: A0010*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0010/

MITRE. (2023x). *ATT&CK asset: A0011*. MITRE ATT&CK®. https://attack.mitre.org/assets/A0011/

MITRE. (n.d.y). *ICS tactics*. MITRE ATT&CK®. https://attack.mitre.org/tactics/ics/

Moneva, A., Leukfeldt, R., & Romagna, M. (2023, December 20). Fieldwork experience researching cybercriminals. I M. Leukfeldt & T. Jansen (Red.), *Cybercrime research in action: Reflections on methods and identity* (s. 435–448). Springer, Cham. https://doi.org/10.1007/978-3-031-41574-6_27

Pedersen, F. A. H., & Jacobsen, J. T. (2024, July 2). Narrow windows of opportunity: The limited utility of cyber operations in war. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyae014

Rid, T. (2014). *Strategic studies: A reader* (2nd ed.). Routledge. https://doi.org/10.4324/9781315814803

Robinson, M., Janicke, H., & Jones, K. (2015, March). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Romagna, M., & Van Den Hout, N. J. (2017, October). Hacktivism and website defacement: Motivations, capabilities and potential threats. *Proceedings of the 27th Virus Bulletin International Conference*. https://scholar.google.com/citations?view_op=view_citation&hl=it&user=-z6SMaQAAAAJ&citation_for_view=-z6SMaQAAAAJ:u-x6o8ySG0sC

Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2022). The nature of losses from cyber-related events: Risk categories and business sectors. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyac016

Singer, P. W., & Friedmann, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. https://books.google.dk/books?id=B88ZAgAAQBAJ

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023, September). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

Tsagourias, N., & Farrell, M. (2020). Cyber attribution: Technical and legal approaches and challenges. *European Journal of International Law, 31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057

TV 2 Nyheder. (2025, 22. januar). *Meget høj trussel om cyberkriminalitet mod danske vandværker*. https://nyheder.tv2.dk/samfund/2025-01-22-meget-hoej-trussel-om-cyberkriminalitet-mod-danske-vandvaerker

Viano, E. C. (2017). *Cybercrime, organized crime, and societal responses: International approaches*. Springer International Publishing. https://doi.org/10.1007/978-3-319-44501-4

Wohlin, C. (2014). *Guidelines for snowballing in systematic literature studies and a replication in software engineering*. Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE '14). https://doi.org/10.1145/2601248.2601268wohlin.eu+1Wikipedia+1

Wu, J. (2012). *Advances in K-means clustering: A data mining thinking*. Springer. https://doi.org/10.1007/978-3-642-29807-3