GÖTEBORGS UNIVERSITET

STATSVETENSKAPLIGA INSTITUTIONEN
CENTRUM FÖR EUROPASTUDIER (CES)

EU: En IT-moderniserad värld, en säkerhetiserad cyberaktör?

- **En empirisk undersökning om nätverksmoderniseringens effekt på EU:s säkerhetsstrategi**

Karl Markus Nefton Svensson

Kandidatuppsats:	15 hp
Program:	Europaprogrammet
Nivå:	Grundnivå
Termin/år:	Ht/2020
Handledare:	Michael Schulz

Abstract

Kandidatuppsats:	15 hp
Program:	Europaprogrammet
Nivå:	Grundnivå
Termin/år:	Ht/2020
Handledare:	Michael Schulz
Nyckelord:	EU, Säkerhet, IT, Säkerhetisering, Cybersäkerhet, 5G
Antal ord:	12 983

The purpose of this study is to analyze whether the EU has undergone a change in its security strategies based on Securitization Theory. I have carried out the survey with the help of official documents and statements from the EU institutions. The process of securitization is based on the constructivist ideas about how actors interact and how an issue can move in the political arena. The survey examines the requirements for a securitization that is included in objectives, actors, and threats as well as implemented measures. I have used a qualitative method to investigate my scientific problem and I will argue that one can answer my question using the criteria contained in the theory. Through my main points in the research, I've come to the conclusion that the EU's cyber strategy has developed from a politicized issue to a securitization issue through the period 2009-2020.

Key words: EU, IT, Security, Securitization, Cyber, Cyber security, 5G

Innehållsförteckning

1. Inledning

Efter andra världskriget präglades de kommande 50 åren av ett kallt krig och det sägs att Internet byggdes för att stå emot nya kärnvapenattacker där det skulle behövas mer än en sårad supermakt för att förstöra vår nya informationsordning. ”Information wants to be free” heter det. Jag nöjer mig med att konstatera att ” Information is free.” (Lindstedt, 2010). Informationstekniken var och förblir ett tillvägagångssätt för att få upplysning om vad som händer i världen. Likt den konkurrens som funnits kring kärnvapen blev strävan efter att vara den främsta aktören inom IT-sfären en ny tävling emellan stormakterna. I dagens samhälle är stora delar av världen beroende av informationsteknik där många av oss lever uppkopplade för att kunna sköta våra dagliga aktiviteter, men hur skyddade är vi? EU-kommissionen presenterade år 2017:

”Aktuella uppgifter visar att digitala hot utvecklas snabbt och att allmänheten uppfattar cyberbrottslighet som ett betydande hot: Medan attackerna med utpressningsprogram har ökat med 300 % sedan 2015, femfaldigades de ekonomiska effekterna av cyberbrottsligheten mellan 2013 och 2017, och kan enligt vissa studier öka med faktor fyra till 2019. 87 % av européerna ser cyberbrottslighet som en viktig utmaning för EU:s inre säkerhet.”
(Kommissionen, 2017: s. 1).

EU:s cybersäkerheten skall bidra till att skydda den europeiska marknaden ifrån externa attacker, identifiera hotbilder, aktörer och figurera i en ledande roll inom den globala världsordningen, där USA, Ryssland och Kina redan infinner sig som andra stormakter. Kommissionens uttalande visar på ett problem som i takt med moderniseringen av nätverk blivit högaktuellt och motsätter sig de kärnvärden som EU:s operationalisering inkluderar. I takt med moderniseringen har en ny spelplan blivit ett faktum där även säkerhetsstrategin krävt nya incitament, men hur har EU:s hanterat och samspelat kring dessa? I den här studien skall jag analysera hur EU:s cyberstrategi sett ut över tidsperspektivet 2009–2020. Då Lissabonfördraget ratificerades 1 december 2009 menar EU att säkerhetspolitiken fått en allt mer kollektiv målsättning. De menar för att en säkerhetsfråga skall kunna lyftas krävs olika sorters strukturer och processer med flera olika aktörers samspel. Fördraget innefattade alltså inte bara att EU:s medlemsstater skall agera kollektivt utan även att de skall erhålla en gemensam röst och identitet när utrikes- och säkerhetspolitik övervägs. (Utrikesrådet, 2020). I vilken mån EU implementerat kollektiva beslut och sedan på ett strategiskt sätt

operationaliserat dem är en delikat debatt som i dagens läge är ytterst primär för unionens säkerhet.

1.1 Syfte och frågeställning

Syftet med den här studien grundar sig på att granska hur EU:s cybersäkerhet utvecklats mellan 2009 (Lissabonfördraget) till 2020 (studiens startpunkt). EU:s säkerhetspolitik är ständigt krävande efter utveckling, både för unionen, dess institutioner och för samtliga medlemsländer. Med tidens tekniska språng har säkerhetsaspekten blivit allt mer relevant kring cyber och IT-säkerhet då den medfört en större spelplan med en större bredd av verksamma aktörer. Uppsatsens syfte kommer därför att således rikta sig emot EU:s implementering och hantering av cybersäkerhetsstrategin där mitt grundläggande syfte skall leda till att analysera en potentiell förändring av EU:s strategikoncept och EU som säkerhetsaktör. För att avgränsa syftet ytterligare har jag formulerat specificerade frågeställningar till min huvudfrågeställning:

På vilket sätt har EU:s cyberstrategi säkerhetiserats under perioden 2009–2020?
I relation till min valda säkerhetsteori, som motiveras i teorikapitlet, valdes följande specificerade frågeställningar som avgränsar huvudfrågan:

- *Hur har EU:s övergripande målsättningarna sett ut kring cyberstrategin?*
  Under den här frågeställningen kommer jag att fokusera på vad EU presenterat för målsättningar och hur de sett ut över tidsperioden 2009–2020.
- *Vilka globala cyberaktörer och hotbilder har EU identifierat?*
  Under den här frågeställningen skall EU:s agerande och identifiering av aktörer och hotbilder presenteras under perioden 2009–2020 med syfte att analysera hur det skiljer sig över tid och de kausala förhållandena till det.
- *Vad för insatser och åtgärder har EU förslagit för att öka säkerheten inom cyberstrategin?*
  Tredje underfrågan skall rikta sitt fokus mot att försöka tolka och analysera EU:s förslagna insatser och åtgärder samt hur en potentiell förändring sett ut över tiden 2009–2020.

2. Tidigare forskning om EU:s cybersäkerhet

I det här kapitlet kommer undersökningen behandla vad vi vet såhär långt om EU:s cybersäkerhet, vad som implementerats och vad olika forskare presenterat för problematik och förändringar inom moderniseringen av nätverk. Då stora delar av den globala välfärden blivit som mest digitaliserad under 2000-talet är forskningen inom cyberteknik och cybersäkerhet fortfarande ett område som det finns mycket att undersöka på, då mestadels av forskningen presenterats under 2010-decciniet och blivit ett allt mer aktuellt ämne med tiden. Upplägget följs upp genom ett strukturerat upplägg av olika rubriker för att främst skilja på den tidigare forskning som resonerar kring EU som cyberaktör, problematiken och nyttan kring medlemsländernas inverkan och slutligen hur nätverksmoderninseringen förändrats, för att kunna förstå hur nya externa hot främjat nya säkerhetsstrategier.

2.1 Cyber och säkerhet – Cybersäkerhet?

Ett perspektiv att se på cybersäkerhet förklaras genom Forskarna Helena Carrapico och André Barrinha (2017) som menar att under de senaste tre decennierna har Europeiska unionen (EU) utvecklats som en säkerhetsaktör. Baserat på olika intervjuer av bland annat europaparlamentet, kommissionen och europeiska ekonomiska samarbetsrådet, mellan 2015–2016 menar de att den transnationella karaktären av säkerhetshoten och de utmaningar som EU identifierat har lett till en progressiv integration mellan interna och externa säkerhetsfrågor. Forskarna poängterar att EU är en invecklad säkerhetsaktör som täcker ett ökande antal områden och policyer, allt från miljö till cyberspace. Ett karakteristiskt drag av denna komplikation har varit EU:s tonvikt på förenandet av intern och extern säkerhet där behovet av att utveckla politik, aktörer och instrument som är sammanhängande, inom den här säkerhetskontexten, krävt en snävare tolkning.

Som erkänt av Jacques Barrot, den tidigare EU-kommissionären med expertis inom rättvisa, frihet och säkerhet menar han att:

”Rättsliga och inrikes frågor (RIF) har i allt högre grad påverkat internationella relationer och spela en viktig roll i Europeiska unionens (EU) externa politik. Omvänt beror många av Europas interna politiska mål på den effektiva användningen av externa politiska strategier”. (Carrapico & Barrinha, 2017: s. 1254).

Forskarna menar alltså att gällande säkerhetsvillkor, terrorism, hybridhot och organiserad brottslighet finns inga gränser. Det här ger kontentan för stramare institutionella kopplingar mellan vår yttre handling och det inre området med frihet, säkerhet och rättvisa i takt med graden av att EU:s säkerhet ökar. Carrapico och Barrinha (2017) yrkar på att frågan bör ställas om samhörighet, som understryker kombinationen av det som nu är en stor mängd instrument, aktörer och politik. EU blir en alltmer komplex säkerhetsaktör men författarna understryker frågan om EU blir allt mer stramare institutionellt, som den påstår sig vara? De menar att det här är en särskilt relevant fråga när man överväger cybersäkerhet. Att erkänna att informationsteknologi blivit ryggraden inom EU har gjort cybersäkerhet till en av de viktigaste säkerhetsprioriteringar. Sådan prioritering har inte bara återspeglats på nivån för nytt initiativ som föreslås, men också i tanken att EU skall eftersträva att bli en effektiv cybersäkerhetsaktör. Det kräver att man måste upprätta en stark samverkan inom unionen och mellan medlemsländerna. Cybersäkerhet ifrågasätter ett antal viktiga dikotomier såsom intern /extern, offentlig/privat, civil/militär) och samtidigt minskar de geografiska skillnaderna mellan nationella, europeiska och de globala nivåerna där säkerhetsområdet är en ideal grund för att bedöma enhetligheten inom EU, menar forskarna.

Carrapico och Barrinha (2017) beskriver den europeiska säkerheten 2016 som markant mindre påstridig än ett decennium sedan och det förklaras genom författaren och forskaren inom internationell säkerhet Allen G. Sens som genom en undersökning 2007 om EU:s politiska utmaningar inom europeisk säkerhet hävdar att *”EU kommer att bli alltmer den institutionella tyngdpunkten för säkerhetspolitisk överläggning, samordning och handling av europeiska regeringar”.* Vilket citeras i (Carrapico och Barrinha, 2017: s. 1267).

Men även om en sådan gynnsam bild av EU:s säkerhetsdelaktighet är långt ifrån fullbordad kan man inte förneka det i områden inom cybersäkerhet, där EU succesivt blivit en stark och viktig aktör. Adderar man sedan de mer komplexa implikationer som hamnar under EU:s ansvar, såsom gränsförvaltning till terrorismbekämpning, blir det klart att ett sammanhängande EU kan vara nödvändigt för att hantera de många säkerhetsfrågor som berör dess medborgare och medlemsstater.

Carrapico och Barrinha (2017) poängterar vikten av att EU bör eftersträva en strukturerad inställning i frågan om enhetlighet inom dess säkerhetsaspekt, med både fokus på de vertikala förbindelserna mellan EU, dess medlemsstater och privata aktörer samt de horisontella

förhållandena mellan dess multipla institutioner och byråer. Med fokus på cybersäkerhet, skriver de att EU har en uttrycklig ambition till att vara en samverkande säkerhetsaktör. EU:s strängare kontroll över medlemsländernas cyberaktiviteter är en prioritet för en ökad samverkan men kan således begränsa enhetligheten om medlemsstaterna väljer att motsätta sig det i allt för bred grad. Debatten om EU:s kollektiva samspel kring cybersäker kan ses som gedigen men medlemsländerna har hittills agerat olika, i frågor som i till exempel reglering av extern IT-infrastruktur. De uppoffringar som krävs för en enhetlig operationalisering har alltså ställt olika incitament emot varandra – Nytta och säkerhet. Hur kan dessa kombineras och till vilket pris?

2.1.1 EU:s cybersäkerhet

Ett perspektiv på hur cybersäkerheten har fått nya incitament förklaras av forskarna J. Scott Marcus och Dr Marieke Klaver (2011) i en undersökning om EU:s systematiska operationalisering för en mer sammanhängande och förbättrad nätverksstruktur samt ett säkrare informationssamhälle. Undersökningen gjordes på begäran av Europaparlamentets ITRE-utskott där huvudfokuset handlade om Europeiska unionens byrå för cybersäkerhet (ENISA). Byrån, som arbetar för att uppnå en hög gemensam nivå av cybersäkerhet i hela Europa, har en målsättning att sträva efter att stärka EU:s cybersäkerhetslag, menar forskarna. Scott Marcus och Klaver (2011) poängterade även, genom en undersökning av EU:s olika implementerade datalagar och direktiv kring cybersäkerhet, att ENISA måste ta sig an de nya utmaningarna som inte var synliga när det bildades 2004. Genom deras undersökning kring ENISA:s operationalisering och funktion identifierade de nya utmaningar i ett ramverk som skulle prägla EU:s framtid från 2011:

- *Genomföra cybersäkerhetsövningar på europeisk nivå och även i samarbete med USA.*
- *Samordna rapporteringen av meddelanden om säkerhetsöverträdelser (och ta emot meddelanden) enligt artiklarna 13a och 13b ramdirektivet (ändrat 2009).*
- *Interaktioner med IT-brottslighet, elektronisk integritet och andra intressenter inom angränsande politikområden.* . (Scott Marcus & Klaver, 2011: s. 4).

Forskarna menar, med det här i åtanke, att ENISA ständigt måste sträva efter att inte bara expandera i organisationsformat utan även inom det internationella samspelet. Genom deras undersökning kring EU:s olika implementerade datalagar och direktiv menar Scott Marcus och Klaver att moderniseringen av informationsteknik och digitaliseringen av säkerhetshot

har kommit att blivit en allt mer primär fråga där utmaningarna från ENISA:s start 2004 tills undersökningens hänvisning 2011 fått ett allt mer bredare perspektiv gällande EU och IT-byråns handlingskraft. Scott Marcus och Klaver (2011) menar att utmaningarna för ENISA:s uppdrag, där risken för en utökad expandering är snabbare än organisationens bemanning, kan leda till en viss tvetydighet i förhållande till IT-brottslighet och integritet.

Det här följdes sedan upp i en undersökning av forskarna Dimitra Markopoulou, Vagelis Papakonstantinou och Paul de Hert (2019) som skriver om EU:s nya cybersäkerhetsram i en finansierad undersökning av Europeiska kommissionens H2020-projekt FORTIKA - Cyber Security Accelerator för betrodda små och medelstora IT-ekosystem. Forskarnas undersökning ledde fram till ett uttalande om att NIS-direktivet är den första övergripande lagstiftningen som genomförs på EU-nivå för skydd av nät- och informationssystem i hela unionen. Markopoulou m.fl (2019) yrkar på vikten av kollektiva skyldigheter som inkluderas av medlemsstaternas inhemska attityder kring deras nationella strategier och hur det påverkar samarbetet på EU-nivå. Ett kollektivt samspel mellan medlemsländerna kan dock medföra en tröghet i operationaliseringen, menar forskarna. För att kunna implementera säkerhetsåtgärder så krävs det en uppoffring. ENISA:s kritiska roll i genomförandet av direktivet, som förstärktes av förslaget till en ny förordning om EU:s cybersäkerhetslag, utarbetar det oundvikliga förhållandet mellan NIS-direktivet och EU:s Allmän dataskyddsförordning. NIS-direktivet publicerades första gången i juli 2016 men trädde i kraft 1 augusti 2018 och innefattar tre delar:

1. *Nationell kapacitet:* EU:s medlemsstater måste ha vissa nationella cybersäkerhetsfunktioner i de enskilda EU-länderna, till exempel att de måste ha en nationell CSIRT (Computer Security Incident Response Team) samt utföra kontinuerliga cyberövningar.
2. *Gränsöverskridande samarbete:* Gränsöverskridande samarbete mellan EU-länder, till exempel EU:s operativa CSIRT-nätverk och den strategiska NIS-samarbetsgruppen.
3. *Nationell tillsyn över kritiska sektorer:* EU:s medlemsstater måste övervaka cybersäkerheten för kritiska marknadsaktörer i sitt land: Förhandsövervakning i kritiska sektorer (energi, transport, vatten, hälsa, digital infrastruktur och finanssektorn) samt övervakning av kritiska leverantörer av digitala tjänster (onlinemarknader, moln och sökmotorer online).

Markopoulou m.fl (2019) menar att deras undersökning lett fram till att NIS-direktivet kan betraktas som ett sent svar på ett redan förvärrat och välkänt problem, vilket även Scott Marcus och Klaver yrkade på redan 2011. Vad som däremot ställer de olika forskarna emot varandra är frågan kring medlemsstaternas roll, då Scott Marcus och Klaver (2011) behandlar det faktum att direktivet ger medlemsstaterna både utrymme för flexibilitet och tid för större eftertanke, vilket kan ses som en motsatt produktivitet, åtminstone om EU:s yttersta mål är att skapa ett område med cybersäkerhet som innefattar en effektiv handlingskraft. Att flera aktörers olika viljor skall samspela om budget, valet av informationsteknik och målsättningar kring vad som är primärt ger cybersäkerheten ett pressat läge, eftersom den kräver effektiva åtgärder omgående. Markopoulou m.fl (2019) följer upp det med att förklara problematiken som expanderat kring cybersäkerhetsincidenter, i form av cyberattacker och till och med cyberkrig, som nu inte bara identifierats på expertnivå utan har också ofta fångat allmänhetens uppmärksamhet. De menar att ett EU-svar i form av NIS-direktivet var försenat med tanke på de många EU-värden som står på spel och i takt med den nya nätverksmoderniseringen har allmänheten kommit att spela en betydande roll för säkerhetsstrategin eftersom de upplevda hoten blivit så pass vardagliga nu även för individen. Det ställer EU i en ny situation där problematiken fått en ny beteckning på EU:s dagordning där kraftiga åtgärder efterlyses ännu mer primärt. För att koppla tillbaka till NIS-direktivet blir valet av rättsligt instrument EU:s svar på en väl genomtänkt och balanserad reaktion som tar hänsyn till cybersäkerhetsproblematik och unionens framtidsplaner för att undvika tröghet i beslutsfattande. Den inrättar nya, permanenta, behöriga myndigheter på medlemsstatsnivå och inför ett system för samarbete över hela unionen. Nationella känsligheter och till och med budgetbegränsningar, liksom olika nivåer av finess inom informationsteknik, beaktas också i texten i NIS-direktivet, i den meningen att det ger medlemsstaterna handlingsutrymme men med den här gången med valet av rättsliga instrument. Markopoulou m.fl (2019) menar att det agerandet kan ses som en fördel snarare än motsatsen och lägger vikt vid att cybersäkerhet är ett kritiskt fält av globalt regleringsintresse. Genom forskarnas undersökning, intervjuer och iakttagelser har man kunnat se hur regleringar förändrats över hela den internationella spelplanen där Kina sedan 2017 infört sin egen cybersäkerhetslag som har givit olika reaktioner inom EU, i takt med det senaste 5G-nätverkets implementering. I samma mån har USA implementerat sin egen cybersäkerhetspolicy. Frågan om datalokalisering, som allvarligt påverkar alla cybersäkerhetsstrategier i relation till NIS-direktivet, borde uppfattas som en

enda bit i ett stort, internationellt pussel, antyder forskarna. Markopoulou m.fl (2019) menar att det kanske är den första EU-biten i spelet, som förhoppningsvis snart kommer att följas, kompletteras och specificeras av många andra i takt med moderniseringen av nätverk och medlemsländernas val och uppoffringar för en effektiv och flexibel strategi.

2.2 Nätverksmoderniseringens effekt på individ och samhälle

Modernisering av nätverk är viktigt att förstå för att nå en grundläggande förklaring varför cybersäkerheten har blivit en ytterst primär säkerhetsfråga. Det förklaras av forskaren Ijaz Ahmad m.fl (2017) i presentationen av 5G-säkerhet: analys av hot och lösningar. Skildringen av IT-innovationerna 1G-5G som trådlösa kommunikationssystem beskrivs som utsatta för säkerhetsproblem redan från början, inom olika nivåer. Ahmads m.fl (2017) studie förklarar problematiken kronologisk. I den första generationen (1G) trådlösa nätverk riktades mobiltelefoner och trådlösa kanalerna mot olaglig kloning och maskering. I andra generationen (2G) av trådlösa nätverk, blev spammeddelande vanligt, inte bara för genomgripande attacker utan även genom falsk information eller implikationen av oönskad marknadsföringsinformation. I den tredje generationen (3G) trådlöst nätverk möjliggjorde IP-baserad kommunikation implementeringen av internet-säkerhetsproblem och utmaningar i trådlösa domäner. Med den ökade behovet av IP-baserad kommunikation aktiverade fjärde generationens (4G) mobilnät spridningen av smarta enheter, multimediatrafik och nya tjänster till den mobila domänen. Ahmad m.fl (2017) menar att det var här IT-hot började bli att mer vardagligt för samhället då den ledde till en mer komplicerad och en dynamisk domän av samlade hot. Med tillkomsten av den femte generationens (5G) trådlösa nätverk har expansionen av säkerhetshot erhållit en rekordnivå av attackvektorer - ett sätt som systemknäckande hackare kan få tillgång till en dator eller nätverksserver där skadligt innehåll sedan kan placeras. Forskarna menar att det således har lett till att säkerhetshotet kommer att vara större än vid tidigare nätverk där oron för integritet och intrång nu lyser starkt på agendan hos allmänheten, med grund i att cybersektorns modernisering av nätverk givit en allt mer bredare marknad och därav medkomna nya hot. Ahmad m.fl (2017) poängterar även att 5G-nätverket inte bara har lett till en kritisk infrastruktur som krävt mer åtgärder för att garantera säkerheten utan även för säkerheten i samhället på individnivå. Forskarna använder intrång i online-nätaggregaten som exempel och menar på att det kan vara katastrofalt för alla elektroniska system som samhället är beroende av.

Ahmad m.fl (2017) menar att 5G kommer att använda mobila moln, SDN och NFV för att möta utmaningar med massiv anslutning, flexibilitet och kostnader. Tillsammans med alla fördelar har dessa tekniker alltså också skapat nya medkommana säkerhetsutmaningar. Det finns ett antal sådana som kan bli mer hotfulla inom 5G såvida de inte behandlas fullständigt och får åtgärder. På grund av den begränsade fristående och integrerade distributionen av dessa tekniker inom 5G kan säkerhetshotvektorerna inte vara helt realiserad. På samma sätt kommer kommunikationens säkerhets- och integritetsutmaningar blir mer synliga när fler användarenheter är anslutna och nya olika tjänster tillhandahålls i 5G. Ahmad m.fl (2017) yrkar även, i sin forskning om 5G och dess hot och potentiella lösningar, att det är högt sannolikt att nya typer av säkerhetshot och utmaningar kommer att uppstå med implementeringen av ny 5G-teknik och tjänster. Med tanke på de här direkta utmaningarna från de inledande designfaserna till distributionen minimeras sannolikheten för en potentiell säkerhet där integritet upphör att gälla när en bred internationell marknad givit externa aktörer en ny form av integration mot EU och dess medlemsländer. Det hotar inte bara samhället i stort utan även individens användning av IT-infrastruktur.

2.2.1 Externa säkerhetshot inom 5G

I takt med att cyberdigitaliseringen fått en svingade expansion i relation till att den globala handeln, har vår värld allt mer integrerad vilket på ett naturligt sätt lockat flera intressenter att genomföra större åtgärder för att nå en topplacering inom informationstekniken. Det menar forskaren Kadri Kaska m.fl (2019) i deras undersökning inom NATO - Cooperative Cyber Defense Center of Excellence som inom Tallin-manualen 2.0 är den mest omfattande guiden kring hur internationellt lag gäller cyberverksamhet. EU:s operationalisering gällande eftersträvan att erhålla rollen som en världsledande cyberaktör har ständig konkurrens av andra stormakter som USA, Ryssland och Kina där den sistnämnde har varit det mest utstående frågetecknet på EU:s agenda sedan den presenterade EU-Kina strategin 2015, menar forskarna.

Kaska m.fl (2019) menar att EU och Kinas interaktioner vilar på en grund av diplomati, handel och säkerhet. En allt mer relevant debatt kring säkerheten och integration har tagit plats de senaste åren då Kinas expandering inom tekniska områden, såsom det ovannämnda 5G-nätverk, har förändrat spelplanen. Potentialen för 5G-nätverk att bli det digitala nervsystemet i samtida samhällen, i relation till Kinas kända förmåga och lust att integrerar

sig i andra världsdelar genom den här funktionen, gör frågan om 5G-distribution mer än bara en teknokratisk fråga – det måste övervägas fullständigt och förstås att valet av teknik har både ekonomiskt och nationella säkerhetseffekter. I deras artikel *”Huawei, 5G and China as a Security Threat”* (2019) förklaras och åberopas telekom-jätten Huawei och säkerhetsproblematiken kring det. Kadri m.fl (2019) skriver att upptrappningen av den nationella säkerhetsdebatten kring Huawei har fångat ett antal 5G-entusiaster. USA, Australien, Nya Zeeland, Japan och Tjeckien har bland annat infört begränsningar för användningen av Huaweis 5G-lösningar på grund av nationella säkerhetsproblem. Större delar av Europa funderar på att följa efter. Sammanfattningsvis är nationernas bekymmer rotade i banden mellan kinesiska kommunikationsteknikföretag och dess underrättelsetjänster som förstärkts av Kinas politiska och juridiska miljö som kräver samarbete med underrättelsetjänsterna. Kaska m.fl (2019) menar att det infinns en rädsla att antagandet av Huaweis 5G-teknik kommer att införa ett kritiskt beroende av utrustning som potentiellt sätt kan kontrolleras av de kinesiska underrättelsetjänsterna och militären under fredstid, men även i kris. Kinesiska teknikföretag har blivit allt mer betydande aktörer på den globala marknaden, med tanke på deras framsteg inom diverse innovationer där särskild förbättrad kvalitet och smidigare kostnader för deras produkter ligger till grund, menar forskarna. Den kinesiska statens legala och politiska inflytande över dess teknikindustri och banden mellan regeringen och företagen lämnar dock de västliga länderna oroliga. Det är ingen hemlighet att Kinas strävan efter av globalt inflytande har stegrat markant i takt med nätverksmoderniseringen och med tanke på landets historia av cyberspionage blir slutsatsen av oroligheter inom EU ett faktum som kvarstår. Kaska m.fl (2019) utvecklar det genom att ingen teknik kan vara helt säker och risken för oväntade sårbarheter som kan utnyttjas av externa aktörer med andra syften kvarstår, vilket måste tas med i beräkningen gällande ett samarbete med externa aktörer såsom t.ex. kinesiska Huawei.

Vidare poängterar forskarna i deras undersökning att kärnan i Huawei-debatten är en omfattande teknikfråga. Det finns hittills ingen allmän bevisning för allvarliga tekniska sårbarheter i specifik Huawei- eller ZTE-utrustning. Som sagt, det är i princip omöjligt att utesluta potentiella tekniska brister som kan utnyttjas i framtiden. Det spelar ingen roll att kinesisk teknik i det här avseendet inte skiljer sig från tillverkad teknik någon annanstans. Huruvida sårbarheter uppstår på grund av avsiktlig handling eller kan utnyttjas på grund av misslyckande (till patchprogramvara eller dålig konfiguration från användarens sida) är av

sekundär betydelse. Det är fortfarande ett problem eftersom upphandling av en viss leverantörs teknik skapar en viss grad av beroende: att skaffa digital teknik handlar inte bara om att skaffa ”ett objekt” utan innebär ett långsiktigt engagemang för en relation med en leverantör, menar forskarna angående nätverksinfrastruktur. Med tanke på dessa förutsättningar är kärnan i Huawei-dilemmat snarare om att bestämma vilken leverantör man kan lita på och vilka mekanismer som bygger ett sådant förtroende på: är det partnerns trovärdighet, verifierbarhet och ansvarighet eller något annat? Kaska m.fl (2019) menar att EU:s operationalisering av cybersäkerhetsstrategi och det kollektiva samspelet mellan medlemsländerna kommer vara av ytterst vikt för att kunna bedöma vilka långsiktiga samarbeten unionen skall främja och avstå ifrån.

Det här summerar de relevanta delarna som tidigare forskning undersökt inom cyberstrategin och säkerhetsaspekten där moderniseringen av nätverk, externa aktörer samt EU:s interna samspel har behandlats. Det interna samspelet ligger till grund för de olika för- och nackdelar med en större kollektiv interaktion mellan EU:s institutioner och medlemsländerna. Det har gjort frågan om cybersäkerheten intressant eftersom alla forskare är överens om en sak – EU måste erhålla en intern flexibel samverkan för att kunna avancera på ett strategiskt plan. Det banar väg för den här undersökningen som riktar sig emot EU:s implementerade cyberstrategi med 2009–2020 som undersökningsperiod, men också baserat på olika tidigare undersökningar, intervjuer och material angående EU:s säkerhet och cyber-attityd, som behandlats i det här kapitlet. Med det här i åtanke kommer mitt bidrag att rikta sig emot att mer ingående analysera hur EU som cybersäkerhetsaktör agerat då tidigare forskning yrkat på stora förändringar inom moderniseringen av nätverk och en expanderad problematik som försatt EU:s interna samspel på sin spets. Har EU:s cybersäkerhetspolitik förändrats i takt med moderniseringen och i så fall, hur och varför? Med tanke på vad tidigare forskning presenterat finns det ett frågetecken kring vilken nivå av cybersäkerhet som EU erhåller. Därför behöver jag ett teoretiskt ramverk för att göra det möjligt att analysera implementeringen och operationaliseringen av strategier och därifrån sätta de i perspektiv. Mitt val blir då Köpenhamnsskolans teori kring säkerhet, vilket aldrig förr applicerats på cybersäkerhet. Kommande teorikapitel kommer förklara, motivera och visa på hur teorin kan appliceras på mitt empiriska material. Sedan ämnar jag undersöka om EU:s cyberstrategi uppfyller de krav som krävs för en fullbordad således kallad - säkerhetiseringsprocess.

3. Teori

Den teoretiska ramen i den här undersökningen kommer att utgå ifrån och inspireras av Barry Buzan, Ole Waever och Jaap de Wildes (1998) teori om securitization (säkerhetisering), som ursprungligen föddes i Köpenhamn och är en del av *”Köpenhamnsskolans teori”* om säkerhetstänk. Anledningen till valet av den benämnda teorin utmynnar i att den förklarar en process som blir primär när ett samhällsproblem blivit så pass omfattande att individen och samhället upplever den som ett vardagligt hot. Köpenhamnsskolans teori om säkerhetisering grundar sig på konstruktivistiska tankar och innefattar olika nivåer och implikationer som krävs för att kunna fullborda en process för säkerhet. För att kunna applicera det teoretiska ramverket på mitt empiriska material krävs en grundläggande förklaring av begreppet säkerhet, konstruktivism och begreppet säkerhetisering för att kunna sätta teorin i perspektiv till uppsatsens fokus om cybersäkerhet och IT-moderniseringen.

3.1 Definition av begreppet säkerhet

Forskaren Gerrard Quille (2004) menar att begreppet säkerhet har genomgått en betydande omvandling och politisk offentliggörande under det sena 90-talet från ett nära militärrelaterad koncept under den tidiga delen av det kalla kriget till en bredare, omfattande och mer samarbetsvillig definition, som representerades i *Helsinki Final Act.* Quille (2004) menar att den europeiska integrationen inom säkerhetssamarbeten har utvecklats till olika politiska EU-instrument såsom militär, handel, utveckling och diplomati. Han menar även att i Europa är det på grund av att européerna har en betydande svaghet i militär kapacitet och den tydliga skillnaden mellan Europas och USA:s attityd kring att använda våld före andra säkerhetsinstrument. Det har bidragit till en effektivitet inom unionens samarbetsprocesser kring den delikata frågan om säkerhet och handlingskraften inom Europa och EU. Västeuropeiska aktörers påverkan, med betoning på Tyskland och Frankrike, har sedan formandet av EU varit starka röster inom EU:s säkerhetspolicy och forskaren Mathias Koenig-Archibugi (2004) förklarar dessa regeringars institutionella preferenser som en förändring av EU:s exterritoriala säkerhetspolicy och betonar att bevarandet av en nationell suveränitet inte är ett mål som delas lika av alla medlemsländers regeringar. Istället har vissa av dem visat på en vilja att främja starka former av politisk integration i Europa. Lusten att upprätthålla staten som en självständig aktör i världspolitiken är en sorts förändringsbar variabel och inte en konstant, menar Koenig-Archibugi. Länken mellan en kollektiv identitet

och regeringarnas politik gäller oavsett om man tittar på allmänhetens identitet eller på ”opinionens ledare”. Styrkan i den regionala styrningen i ett land är starkt relaterad till regeringens preferenser när det gäller sammanställning av suveränitet och delegering i utrikesfrågor. Det här ger implikationer av att de olika medlemsländernas inhemska attityd till den gemensamma utrikes- och säkerhetspolitik som bedrivs av EU, blir en bredtolkad aspekt i flera avseenden. Medlemsländernas samverkan kring den kollektiva säkerheten har stark påverkan av den nationella attityden vilket sedan EU:s födelse varit en stor utmaning då medlemsländerna inte alltid är överens. Quille (2004) och Koenig-Archibugi (2004) pekar alltså båda på den kollektiva identiteten som en av de starka faktorerna kring säkerhet, med rot i medlemsländernas nationella beteenden och ageranden. För att kunna knyta an de båda forskarnas åsikter till säkerhetskonceptet menar de att om inte det kollektiva samspelet anammas kommer inte heller säkerhetspolitiken nå någon form av slagkraft. Redaktionen för EU-upplysning som bedrivs och förvaltas av Myndigheten för samhällsskydd och beredskap (MSB) poängterade att:

> *”Grundtanken är att ett lands säkerhet byggs i samverkan med andra. Men också att länderna idag i EU är så integrerade och beroende av varandra att det knappast är möjligt för övriga EU-länder att ställa sig neutrala om ett medlemsland hotas. Fördraget medför även en gradvis utveckling av en gemensam försvarspolitik, som enligt fördraget kommer att leda till ett gemensamt försvar.”* (MSB, 2010).

Myndigheten (2010) menar att det ligger en solidaritetsklausul till grund för en kollektiv samverkan kring EU-policy som rör utrikesfrågor och säkerhetspolitik. En allt mer integrerad global värld har medfört olika frågetecken kring ny problematik, riskbedömningar och samspel inom unionen. Står Europa och EU enat kring cybersäkerheten? Låt oss börja med Christian Rues-Smith (2009) förklaring av konstruktivismen, för att därifrån förstå hur en stat eller union kan enas kollektivt och erhålla kapacitet att operationalisera förändringar inom säkerheten.

3.2 Konstruktivismen

Det finns olika inriktningar inom konstruktivismen men alla har del i en och samma grundläggande ontologiska uppfattning om hur det sociala livet ser ut och ett större förklarande än de *”rationella teorier”* som setts mer som traditionella. Konstruktivismens

teori bygger på att alla intressen är konstruerade för att få aktörer att uppfatta en specifik situation och agera utifrån den. Till skillnad från realismen lägger inte en konstruktivist något värde i vilken makt en aktör innehar, eftersom det är ett konstruerat värde som endast bedöms av andra aktörer. (Rues Smit, 2009: s. 220).

*”Enligt det konstruktivistiska perspektivet – och i motsats till realismens synsätt – är verkligheten en konstruktion som inte refererar till något objektivt som existerar oberoende av det sociala” (*Justesen, Mik-Meyer, 2011: s. 22).

Låt oss säga att ett land innehar en stark militant makt. Enligt konstruktivismen kan enbart att land med stark militant makt uppfattas som en stark aktör om andra aktörer känner sig hotade och därav definierar det specifika landet som stark militant makt. Det sammanfattas genom att ett värde är ständigt växlande men kan också vara en konstant över en längre tid. (Soltani m.fl, 2014. s. 154). I Soltanis m.fl (2014) presentation av konstruktivismen beskrivs forskaren Christian Rues-Smits idéer där han menar att nya konstitutionella värden växer ut ur djupa ontologiska förändringar i människans medvetande. Han pekar även på villkoren för en legitim styrning i kärnstater. Kärnstaterna överför dem till andra delar av världen. Dessa metavärden blir sedan gradvist mer strukturella drag i det internationella samhället. (Soltani m.fl, 2014. s. 155). Det grundläggande konstruktivistiska synsättet är grundat på strukturer. Det är strukturer som bildar en aktörers sociala eller politiska handlingssätt vilket inkluderas för både individ och stat. Utöver de materiella strukturerna kan alltså både de normativa och idémässiga strukturerna ses som kausala eftersom intressen alstras i de egenintressen som har sin grund i identiteter, normer och idéer. Gemensamma idéer och värderingar kan ses som strukturella vilket ger kontentan av en robust påverkan för både det sociala och politiska handlandet. Konstruktivismen menar att när en stat och dess befolkning ser sig själva som en gemensam enhet med delande normer och uppfattningar främjas en operationaliseringsgrund som gör det möjligt att arbeta tillsammans och forma en gemensam identitet. Kopplar man det till dagens samhällen kan man se det ur olika perspektiv. Det ena är att det sker mycket sällan då även en nation har olika inneboende identiteter men oftast med ett grundläggande normsystem och regelverk vilket formar en sort social identitet som landet förespråkar internationellt. Det andra är en sammansatt gemenskap, såsom EU, där den gemensamma enheten inkluderas av medlemsländernas vilja och ambition att sträva efter kollektiva målsättningar. (Reus-Smit, 2009: s. 220–225).

De alternativa ickemateriella strukturerna är även de relevanta för konstruktivismen eftersom de är med och formar en politisk aktörs sociala identitet. Dess kausala funktion har stor betydelse för att kunna begripa hur aktörers identiteter influeras och även hur aktören agerar. En viktig beståndsdel inom konstruktivismen är alltså att förstå hur aktören utvecklar ett specifikt intresse och identifierar det för att eftersträva handlingskapacitet. Med andra ord så menar konstruktivismen att fokus ligger på formandet av de här identiteterna eftersom en aktörs sociala identitet formar en aktörs intresse. Med det i åtanke förstås vikten av strukturer enklare och för att ta det ytterligare ett steg så menar en konstruktivist att det här är ömsesidigt format. Eftersom diverse strukturer figurerar kausalt gällande aktörers intressen och identiteter blir kunskap det faktum som är grundläggande för att förstå aktörens koncept. När individen känner sig hotat skapas ett intresse och en medvetenhet, vilket senare bär frågan högre upp på dagordningen. Om frågan blir så pass omfattande att en större samling individer upplever hotet krävs åtgärder av det politiska etablissemanget för att undvika maktförlust. De konstruktivistiska tankarna har ett flertal orienteringar men rotas i att allting får sin innebörd i en social kontext där fenomenet existens värderar och handlar. Som nämnt ovan är det alltså hur saker och ting uppfattas som är föränderliga med faktorer som kunskap, intressen och identiteter och konstruktivismen menar att det är faktumet som gör att olika aktörer upplever saker olika. (Reus-Smit, 2009: 220–225).

3.3 Köpenhamnsskolans teori om säkerhetisering

Forskaren och författaren Michael Sheehan (2005) gjorde en undersökning om de olika positioner som diverse forskare har intagit för tolkning av säkerhet och han förklarar att en konstruktivist menar att säkerhet som begrepp är någonting som är socialt konstruerat, vilket i sin tur har en unik social innebörd. Som nämnt ovan är det beroende på vem, vad eller i vilken tidperiod som begreppet definieras. Utfallen blir olika eftersom när tiden går förändras samhället och den sociala kontexten. (Sheehan, 2005: s. 43). Inom undersökningens teoretiska aspekt kring säkerhet blir Köpenhamnsskolan ett användbart teoretiskt verktyg där de har specialiserat sig på säkerhetsperspektivet och menar att fler områden skall ses genom en säkerhetsorienterad synvinkel om så krävs. Den yttersta aspekten gällande säkerhetsagendan och den mest betydande anledningen till att det är relevant utmynnar i att en expanderad säkerhetsagenda ger en större omfattande handlingsplan för diverse problemkomplex, som annars kommit i skymundan. Sheehan menar att eftersom det traditionella synsättet på

säkerhet enbart riktat sig emot den militära sektorn ger nu istället den mer omfattande säkerhetsagendan en chans till att andra frågor skall få mer utrymme och även åtgärder. (Sheehan, 2005: s. 3).

En mer omfattande säkerhetsagenda är en primär grund för att kunna agera kring andra åsidosatta frågor, där den relativt nya problematiken kring cybersäkerheten infunnits. Buzan m.fl menar att olika sorters säkerhetsfrågor är intressanta och inte bara rationalisternas tankar kring att säkerhetsfrågor definieras genom krig. Köpenhamnsskolans teori om säkerhet har format en grund för säkerhetsaspekten och menar att det är en slags politik som går att sätta i perspektiv på ett flertal områden med en klar bild av att säkerhet är något nödvändigt som stabiliserar, då det råder konfliktinfekterad stämning. (Buzan m.fl 1998: s. 4). De menar att man inte bara kollar på statens säkerhet utan individen i sig, det vill säga *human security*. För att applicera det på cybersektor så tolkas det genom att cybersäkerhet är staten och folkets säkerhet. Buzans m.fl teori om säkerhetisering är applicerade på fem olika sektorer och tre analysnivåer, där bland miljösektorn och den militanta sektorn. (Buzan m.fl 1998: s. v). Säkerhetiseringen som teori förklaras som en process där det används som ett analytiskt verktyg med syfte att förklara en potentiell förändring inom aktuella politiska frågor. Säkerhetiseringsprocessens trestegsmodell är en givande nyckel för uppsatsen då de olika faserna ämnar förklara om och i så fall hur EU förflyttat sig inom den utvalda sektorn (cybersektorn). Trestegsmodellen går emellan en icke-politiserad fråga till en säkerhetsfråga. I boken presenteras de tre olika faser genom:

- *Den icke-politiserade fasen*
- *Den politiserade fasen*
- *Säkerhetiseringsfasen*

Den första fasen förklaras genom att en fråga är avgränsad till den samhälleliga basen utan samspel eller interaktion av den offentliga eller politiska debatten. Om fokuset kring frågan ökar förflyttas den till nästa steg där den nu politiseras och erhåller större politiskt fokus. Säkerhetiseringen är det slutgiltiga steget vilket implementeras när frågan har kommit att bli så pass känslig och äventyrande av samhällets överlevnad att det krävs effektiva och krävande åtgärder. Buzan m.fl menar att säkerhet är något negativt och uppstår när en politisk aspekts funktionella syfte blir för känsligt och utsatt. (Buzan m.fl 1998: s. 23–24).

Det är viktigt att tillägga att de tre olika faserna inte är totalt orörliga, det kan ses som problematiskt att veta och påvisa när en fråga blivit säkerhetiserad och det är därför processen skall ses som ett analytiskt verktyg till att analysera ett händelseförlopp och därifrån kunna dra olika slutsatser. Säkerhetiseringsprocessen definierar tre olika aktörer som gör det möjligt för analysen att knyta an till säkerhetsteorin. Nedanför i *Tabell 1* har säkerhetsteorin applicerats på cybersäkerheten där olika aktörer definieras i relation till cybersäkerheten.

Tabell 1. Analysschema.

	Referensobjekt	**Säkerhetiseringsaktör**	**Funktionell aktör**
Teori	Aktören som är existentiellt hotad med legitima krav på bevarande.	Genomför säkerhetiseringen genom att klargöra vad som är existentiellt hotat.	Influerar dynamiken inom en säkerhetssektor utan att vara något av de tidigare alternativen.
	EU:s medlemsländers säkerhet	**EU:s institutioner**	**Externa aktörer inom cybersfären**
Empiri	T.ex. Bevarandet av de nationella förhållandena och tillvaro – Medlemsländernas säkerhet.	Genom EU:s institutioner kan politiska förändringar implementeras.	Externa aktörer som identifierats av EU som hot mot cybersäkerheten.

Referensobjektet och *säkerhetiseringsaktören* kännetecknas genom EU:s interna samarbeten medan den sistnämnda *funktionella aktören* förklaras av Buzan m.fl som den aktör som indirekt inverkar på säkerhetsdynamiken utan att erhålla rollen som någon av de föregående aktörerna. I relation till cybersäkerheten är området inte definierat inom säkerhetsteorin, såsom sektorerna inom klimat- och miljöhot är, där funktionella aktörer kan ses som till exempel förorenade företag. Cybersäkerhetens funktionella aktörer blir då de externa hot utanför unionen som påverkar de dynamiska säkerhetsförhållandena på ett oroväckande sätt. (Buzan m.fl 1998: s. 36, 52–57).

Köpenhamsskolan menar att det krävs en instudering av en politisk diskurs för att kunna analysera en säkerhetisering där ett argument med underhåll av en specifik retorik resulterar till att en publiks tolerans förändras och därifrån ger makthavaren en möjlighet att gå förbi delar av implementerade föreskrifter, som annars skall efterföljas. (Buzan m.fl 1998: s. 25).

Waever (1998) förklarar säkerhetiseringsprocessen som en *”speech act”* och menar att skapandet av säkerhetsfrågor rotas i en diskurs med anknytning till överlevnad, hot och risker. Förskjutningen från att en fråga blir ett säkerhetsproblem sker när en elit (kan vara varierande) presenterar en hotbild mot säkerheten och det är själva presentationen som blir *”the speech act”*, men en speech act kan även innefatta hur individer samtalar om ämnet. Han menar att grunden till ett säkerhetsproblem bygger på aktens presentation och dess effekter och inte nödvändigtvis om säkerhetshotet ses som reellt eller inte. (Buzan m.fl 1998: s. 26–27).

Med det sagt så förklaras synen av säkerhetisering inom Köpenhamsskolan med ett poängterande intresse av hur dess processen influerar den politiska agendan genom olika effekter. De åtgärder som görs möjliga i samband med en säkerhetiseringsprocess formas genom att benämningen av säkerhet bildar en diskurs med grund i en existentiell skräck. Därifrån kan en förskjutning ske från den politiska arenan genom att statsrepresentanterna kan legitimera de planerade åtgärder som anses nödvändiga för att kunna försvara sig. Med det här i åtanke blir handlingskraften av en säkerhetisering harmlös om den inte får support från det politiska etablissemanget. Efter att hotet presenterats krävs det acceptans för att kunna vidta de åtgärder som krävs. Det som skiljer en säkerhetisering från ett säkerhetiseringförsök blir således att en fullbordad säkerhetisering kräver mandat ifrån den styrande makten. (Buzan m.fl 1998: s. 25)

Köpenhamnsskolan tre komponenter som kännetecknar en lyckad säkerhetisering identifieras genom: existentiella hot, krisåtgärder samt skiftandet av förekommande lagar, där det slutgiltiga målet skall resultera i en lägesändring av samspelet emellan olika grupperingar. Slutligen så poängterar Köpenhamnsskolan vikten av det politiska syftet kring förskjutningen av en sakfråga från presentation till toppen av den politiska dagordningen. Smidandet från en konstruktion till legitimeringen av åtgärder skall ses som det specifika intresset. Buzan m.fl. beskriver det här som *”beyond the established rules of the game”*.(Buzan m.fl 1998: s. 23-26).

Nedan följer uppsatsens metodkapitel som skall ge svar på vilket empiriskt materialet som skall tillämpas och hur det skall analyseras i relation till Buzan m.fl (1998) säkerhetiseringsteori. Slutligen kommer det teoretiska perspektivet diskuteras utifrån de olika

fasernas som presenterat för att därifrån kunna granska om EU genomgått någon form av säkerhetisering inom en ny form av cybersektor.

4. Metod

Den här uppsatsens ambition ämnar undersöka EU:s säkerhetsstrategi, målsättningar och vad som implementerats kring cyberfrågan för att förstå hur EU:s säkerhetspolitik har implementerats i relation till moderniseringen av informationstekniken. Genom en presenterad förförståelse om hur EU:s säkerhetsstrategi sett ut blir det slutgiltiga mål att undersöka vilka strukturer som infunnits kring cybersäkerheten och relevanta skillnader, med det teoretiska perspektivet som underlag. Studiens undersökningsdesign grundar sig på en kvalitativ innehållsanalys. Den sortens metod är mest effektiv för att undersöka hur EU:s cyberstrategi har sett ut från 2009 till 2020 eftersom den ämnar söka efter olika nyckelfaktorer i politisk strategiimplementering och sätta det i perspektiv till säkerhetiseringsprocessen. I den kvalitativa innehållsanalysen skall olika teman definieras med tanke på att det inte är något specifikt som räknas i den här analysen. Om huvudsyftet är att finna mönster i större textmängder, jämföra olika sorters texter eller dokument från olika tidpunkter används många gånger en innehållsanalys. (Bergström & Boréus 2012: s. 50–51). Med tanke på att dokumenten har en bred tolkning så kommer en operationaliseringstabell bidra till en större smidighet gällande vad jag skall söka efter och vad som skall belysas. Genom en kodningsinstruktion kommer sedan olika politiska implikationer kategoriseras för att sedan kunna tolkas vidare genom en gardering av teman - målsättningar, aktörer, hotbilder och implementerade åtgärder (specificerade frågeställningarna). Efter att jag har identifierat olika värdeladdade enheter så kan jag börja se hur det sett ut över tid. En viktig faktor i det här fallet är vetenskaplig kumulativitet. Det är essentiellt och menar att den här analysens forskning skall kunna samverka med annan forskning runt samma ämne för ökad och effektivare kunskap. En annan viktig poäng som analysen skall ha i åtanke är att analysera de olika uppsättningar av texterna och dokument parallellt för att undvika systematisk glidning, där resultatet kan ge att de båda texterna bedöms olika. Istället har texterna bearbetats fram och tillbaka där de systematiska glidningarna blivit minimala för resultatet. (Bergström & Boréus. 2012, s. 52–58).

4.1 Material

Det empiriska materialet jag valt att använda mig av är sex olika dokument/offentliga uttalanden. Anledningen till valet av ett flertal dokument grundar sig på att chansen skall finnas att förstå vad som skett över tid och hur det ser ut idag. Uppsatsen eftersträvan handlar

om att över en 10–11 års period förstå vad som skett inom EU och varför, med tidigare decennium i åtanke, då den här perioden varit mest influerad av modernisering av nya IT-incitament. Uppsatsens valda offentligt publicerande dokumenten och uttalanden sträcker sig från slutet av 2000-talet decenniet och över hela 2010-decenniet. Det första dokument är *”*Europeiska unionens råd: ”En europeisk säkerhetsstrategi. *Ett säkert Europa i en bättre värld”* (2009). Där presenteras en uppdaterad säkerhetsstrategi i samband med att Lissabonfördrag ratificerades samma år och EU fick en ny vändning inom säkerhetens kollektiva samspel. Det andra dokumentet är också ett strategidokument där kommissionen presenterar ”EU:s strategi för cybersäkerhet: *En öppen, säker och trygg cyberrymd”* (2013). Det här var det första omfattande strategidokumentet kring cyberstartegin. Det tredje dokumentet är ett pressmeddelande från kommissionen. Kommissionen (2017) *”Unionens tillstånd. Kommissionen förstärker EU:s svar till cyberattacker.”* Syftet med det här dokumentet är att poängtera hur EU själva uppfattade deras tillstånd under den här tiden. Det följs upp av ett briefingdokument från europeiska revisionsrätten - *”Utmaningar för en ändamålsenlig EU politik för cybersäkerhet”*(2019). Det dokumentet blir en nyckel för att förstå vad som håller på att hända inom unionen efter att problematiken fått ännu mer ljus efter kommissionens uttalande 2017. *”Förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater”* presenteras också och förklarar bland annat vilka åtgärder EU lyckats med och hur det operationaliserats. Slutligen och samtidigt mest nyligen kommer kommissionens presenterade strategidokumentet *”*Säker 5G-utbyggnad i EU – *Genomförande av EU:s verktygslåda.”* (2020). Här kommer vissa nyckelaktioner av EU presenteras och hur de kan knyta an till en ny säkerhetsstrategi. I vilken mån materialet tolkas kan ses med kritiska ögon ibland då det krävs intersubjektivitet för att uppnå en opartisk och distinkt förklaring av händelseförlopp och inspelande faktorer. I fråga om annat material som kunnat vara aktuellt för undersökningen gjordes en avvägning kring vad som var mest nyttigt för att kunna bevara uppsatsens precision och samtidigt hålla undersökningens tidsram, samtidigt som problemformuleringen behandlas i mest svarsenlig mån. Om jag hade använt mig av de dokument som utgick, som främst innefattar EU:s diplomati, tror jag riktningen på mitt resultat hade resulterat till ännu mer fokus på EU:s diplomatiska attityd och mindre fokus på vad som implementerats kring cyberstrategin och det interna samspelet mellan EU och medlemsstaterna. Med tanke på att EU inte bara spelar ett politiskt spel med medlemsländerna utan även med externa nationer finns det risk att

analysen blivit för omfattande kring hotbilder och aktörer och det hade kunnat resultera i för mycket fokus på just den aspekten. Med andra ord hade den förskjutit för mycket fokus från EU:s inhemska målsättningar och åtgärder. Uppsatsens fokus ligger främst på hur EU:s samspel med medlemsländerna och hur unionen agerat för att effektivisera säkerhetsprocessen genom ett kollektivt samspel kring hot och aktörer. De bortvalda dokumenten öppnar dock upp för vidare forskning där till exempel en *case study* (fallstudie) är ytterst intressant eftersom Huawei och Kina är i framkanten inom nätverksinfrastruktur och strävar efter en större integration i Europa. Det här stärker uppsatsens vetenskapliga kumulativitet.

4.2 Etiska övervägande

Etiska övervägande, som främst riktar sig emot om forskningen kan skada någon, tolkas som i god mån. Anledningen till det är för att uppsatsen använt sig av offentligt publicerade dokument vilket allmänheten har tillgång till. Det gör att det empiriska underlaget finns till hands för uppföljning och vidaretolkning av min forskningsfråga. Etiska ställningstagande som infinns i innehållsanalys grundar sig på den europeiska kodexen för forskningens integritet där principerna för en god forskningssed ses som – *Tillförlitlighet, Ärlighet, Respekt och Ansvarighet.* Den kvalitativa innehållsanalysens design är konstruerad på det sätt att kunna ge den mest givande och pålitliga bilden av det jag skall undersöka. En bred resursanvändning och ett flertal offentligt publicerade dokument av EU:s institutioner ligger till grund samt offentligt publicerade artiklar med godkända intervjuer, från början av 2000-talet enda till 2020. Allmänheten har full tillgång till allt material vilket formar en *tillförlitlighet*. *Ärlighet* och *respekt* blir ett faktum genom att ingen information från dokumenten snedvrids utan min objektiva tolkning av dokumenten, artiklar och andra faktakällor är i linje med det som presenteras i dokumenten. För att inte forskningen skall skada någon eller sända felaktiga budskap eftersträvas således även *ansvarighet* från idé till publicering där uppsatsens författare står för publiceringens ansvar och dess konsekvenser, för att kunna bidra till en legitim bild och potentiell utbildning inom det berörda området. (ALLEA, 2017: s.4).

4.3 Analys av datamaterial

Analysen av det empiriska datamaterialet kommer att analyseras genom följande exempelstruktur i *Tabell 2* där de specifika dokumentens syfte är att presentera ett svar som

förklarar mer precist var EU står i frågan under det specifika året. Därifrån kan vad som presenterats kopplas till EU:s tillfälliga säkerhetiseringsfas för att forma en struktur kring hur unionen har behandlat cybersäkerhetsstrategin över tid. Nedan förklaras vad för data som har hämtats och hur det sätts i perspektiv till de specificerade frågorna.

Tabell 2. Operationalisering av cyberstrategins säkerhetiseringsfas

Frågeställning	Exempel på nyckelmening	Dokument	Säkerhetiseringsfas
Hur har EU:s övergripande målsättningarna sett ut kring cyberstrategin?	*”Öka medvetenheten och förstärka det internationella samarbetet.”*(s. 14.)	Europeiska unionens råd: ”En europeisk säkerhetsstrategi. *Ett säkert Europa i en bättre värld”* (2009).	*Den politiserade fasen*
Vilka globala cyberaktörer och hotbilder har EU identifierat?	*”Ökningen av ekonomiskt spionage och statsunderstödda aktiviteter inom cyberrymden utgör en ny kategori av hot för myndigheter och företag inom EU.”(*s. 3)	Kommissionen: EU:s strategi för cybersäkerhet: *En öppen, säker och trygg cyberrymd”* (2013).	*Den politiserade fasen*
Vad för insatser och åtgärder har EU förslagit för att öka säkerheten inom cyberstrategin?	*”Vi måste arbeta tillsammans för att stärka vår resiliens, skynda på den tekniska innovationen, stärka de avskräckande effekterna, stärka spårbarhet och ansvarsskyldighet samt utnyttja internationellt samarbete för att främja vår gemensamma cybersäkerhet”.* (Julian King: s. 1)	*”Unionens tillstånd. Kommissionen förstärker EU:s svar till cyberattacker.”* (2017)	*Den politiserade fasen* -> *Säkerhetiseringsfasen*
På vilket sätt har EU:s cyberstrategi säkerhetiserats under perioden 2009–2020?	*”Europeiska unionens råd har antagit denna förordning.”*(s. 1)	”Förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater”	*Säkerhetiseringsfasen*

5. Analys av EU:s cybersäkerhetsstrategi

Nedanstående kapitels syfte har som ambition att svara på huvudfrågeställningen: *På vilket sätt har EU:s cyberstrategi säkerhetiserats under perioden 2009–2020?* Med hjälp av de specificerade frågeställningarna och Buzans m.fl (1998) säkerhetiseringsteori skall det empiriska materialet försöka besvara vad som skett inom EU:s cyberstrategi och om den genomgått någon form av fullständig säkerhetiseringsprocess. De utvalda dokumenten kommer presenteras i en kronologisk ordning under varje specificerade frågeställning för att i smidigast mån kunna analysera vad som skett över tid. Målet är att analysera resultatet av vad som presenteras i de utvalda dokumenten och pressmeddelanden med tidigare forskning och teoretiska perspektiv i åtanke. Sedan skall analysens syfte gå till grund med om det skett några övergripande strukturella förändringar inom unionens cybersäkerhetspolitik i en diskussion om hur EU och medlemsländernas sampel sett ut.

5.1 EU:s övergripande målsättningar

Frågeställning som ligger till grund för den rubriken är således:

Hur har EU:s övergripande målsättningarna sett ut kring cyberstrategin?
EU:s övergripande målsättning kring unionens cyberstrategi har fått en omfattande vändning över tid när det kommer till säkerheten. I ”Europeiska unionens råd: ”En europeisk säkerhetsstrategi. *Ett säkert Europa i en bättre värld”* (2009) poängterades vikten av en sammansättning och implementeringen av en gemensam EU-strategi, där ökad medvetenhet och ett förstärkt internationellt samarbete skulle ligga till grund för ett kommande decenniet. Trots en omfattande behandlad säkerhetsstrategi infanns enbart en kort del om IT-säkerheten och EU-rådet yrkade på en målsättning att iscensätta en ny analys gällande cyberhoten för att kunna handla mer effektivt kring området. (EU-rådet, 2009: s. 13–14). För att koppla det till EU:s målsättningar inom cyberaspekten blir kommissionens presentation om ”EU:s strategi för cybersäkerhet: *En öppen, säker och trygg cyberrymd”* (2013) mer lönsam där de nu presenterade en ny form av målsättningar som inkluderar skyddandet av grundläggande rättigheter, yttrandefrihet, personuppgifter och sekretess. En tillgänglighet för alla med fokus på ett demokratiskt och effektivt styre av ett flertal intressenter där det gemensamma ansvaret för att garantera cybersäkerheten nu blivit ett primärt mål inom unionens säkerhetsstrategi. (Kommissionen, 2013: s. 4) EU:s agerande hade nu från 2009 till 2013 gått mot ett större

fokus kring det kollektiva ansvaret men fortfarande med relativt vag styrning gällande operationalisering eftersom handlingskraften förblev utspridd och ostrukturerad. Buzan m.fl. menar att den konstruktivistiska synen bygger på att gemensamma idéer och värderingar kan ses som strukturella vilket påverkar både det sociala och politiska handlande. EU:s hade under perioden 2009–2013 förändrat inställningen till tydligare gemensamma idéer men hade fortfarande en avsaknad av effektiv handlingskraft då säkerhetsproblematiken kring moderniseringen av den nya informationstekniken inte visat sig vara tillräckligt bearbetad. (Reus-Smit, 2009: 220–225).

I takt med att informationstekniken expanderade och med det även cyberattackerna presenterade kommissionen (2017) *”Unionens tillstånd. Kommissionen förstärker EU:s svar till cyberattacker.”* Uttalandet påpekade en stark anknytning till nya EU-incitament om cyberstrategin där nya verktyg, såsom en europeisk IT-säkerhetsmyndighet och ett ansvarsfullt statligt agerade skulle ligga till grund, med tillämpningen av internationell rätt och ett ansvar på EU-länderna att ta itu med utmaningarna och hoten tillsammans då de nu uppfattats så pass omfattande och riskartade av samtliga medlemsländer. (Kommissionen, 2017: s.1) Kommissionen förstärkte här tankarna kring resiliens och att det nu skulle vara fokus på att påskynda den tekniska innovationen, inte bara med ett europeiskt fokus kring att ligga i framkant utan nu även för säkerheten. Höga IT-säkerhetsstandarder skulle vara företagens nya konkurrensfördel för att utifrån en stark privat sektor kunna införliva ett starkt EU där medlemsländerna erhåller en hög lägstanivå inom IT-säkerhet, med syfte att därifrån kunna ta expanderande steg mot ett mer internationellt samarbete på lika villkor. I överenstämmelse med Buzans m.fl socialkonstruktivistiska förankrade teori kan man säga att det var här som cybersäkerheten gick emot en säkerhetiseringsprocess inom målsättningarna. Kommissionen poängterade nu vikten av en omfattande kollektiv säkerhet kring cybersfären och dess aktörer. Kommissionen och EU:s andra institutioner hade omformats till en mer säkerhetiseringsaktör med fokus på att förenkla och främja en effektivitet och flexibilitet bland unionens medlemsländers inhemska operationalisering av cybersäkerheten. Det räckte inte med att man delade samma målsättningar, utan det krävdes även att EU kunde operationalisera på ett nytt plan. Cybersäkerheten ansågs utgöra ett hot som globalt trappats upp med stor politisk betydelse, vilket europeiska revisionsrätten förklarade i *”Utmaningar för en ändamålsenlig EU politik för cybersäkerhet”*(2019). Här presenterades en målsättning som skulle rikta sig emot en ökad transparens i form av detektering och rapportering, för att

slutligen kunna iscensättas av en samordnad hantering mellan EU:s institutioner och medlemsländer. Ökade resurser, som är en vital del för säkerhetiseringsprocessen, behövdes här för att kunna undersöka allvaret, enligt revisionsrätten. (Revisionsrätten 2019: s. 7, 33).

Buzan m.fl menar att en del av teorin är att en säkerhetisering skall förankras hos befolkningen och medlemsländerna *(referensobjektet)* där de måste ge sitt godkännande (Buzan m.fl 1998: s.31) och det fick en omfattande förändring i samband med kommissionens presenterade strategidokumentet *"*Säker 5G-utbyggnad i EU – *Genomförande av EU:s verktygslåda."* (2020). I takt med den senaste informationsteknikens uppsving (5G) nådde målsättningarna sin yttersta kraft då medlemsländerna genomförde en grundläggande riskbedömning av IT-säkerheten som främjade ett enklare och stadigare samarbete för en EU-operationalisering av cyberstrategin säkerhetsåtgärder.

Det här antyder på att EU:s målsättningar har under perioden 2009–2020 sett en större förändring över tid. Förändringen i sig har varit en process som rotats i ett kollektivt ansvar med ett första fokus på EU:s institutioner men som sedan förskjutits allt mer med större fokus på en nedbrytning av problematiken och medlemsländernas specifika riskbedömningar. Att medlemsländerna setts enligt Buzan m.fl som referensobjektet är inget häpnadsväckande men däremot har säkerhetiseringsaktören breddats mer från att EU handlar på en intersubjektiv nivå, till att bearbeta samarbetet med medlemsländerna till ett större kollektivt ansvar kring rollen som säkerhetiseringsaktör. Problematiken som dock infunnits sig har varit att i takt med att EU försökt expandera säkerhetsstrategins målsättningar har medlemsländerna haft diverse motsättningar och det är anledningen till att processen har behandlats med en viss tröghet. EU har handlat i takt med att problematiken expanderat av IT-hot men dock inte förrän 2020 skedde en samordnad organiserad riskbedömning från medlemsländerna som skulle kunna skett i tidigare mån, vilket förklaras mer ingående i nästa frågeställning.

5.2 Globala aktörer och hotbilder

Frågeställning som ligger till grund för den rubriken är således:

Vilka globala cyberaktörer och hotbilder har EU identifierat?

EU:s bild av cybersäkerhetens hot och aktörer och hur de har identifierats spelar en stor roll för att på ett grundläggande sätt kunna implementera en säkerhetsstrategi som bryter ned och förklarar de faktorer som varit till fog för problematiken.

I ”Europeiska unionens råd: ”En europeisk säkerhetsstrategi. *Ett säkert Europa i en bättre värld”* (2009) valde europeiska rådet att rikta sitt fokus mot hotbilden som utgjordes av attacker mot privata och statliga IT-system i EU:s medlemsstater. En större problematik som behövdes mer upplysning kring, menade rådet. (Rådet 2009: s. 13–14). Redan 2009 hade den markanta ökningen av cyberattacker ställt EU i en situation där det krävdes aktiva åtgärder och identifiering av hotbilder och aktörer, för att effektivt kunna fortsätta att utveckla ENISA och stärka de andra IT-myndigheterna mot flera angrepp. I kommissionens *”*EU:s strategi för cybersäkerhet*: En öppen, säker och trygg cyberrymd.”* (2013) identifierar EU en bred upplaga av hotbilder som mer övergripande riktade sig emot ekonomiskt spionage, statsunderstödda aktiviteter samt stater utanför EU som missbrukar cyberrymden för att övervaka och kontrollera sina medborgare. Fokuset kring identifieringen av olika sorters hot stärktes nu av olika aktörsbilder där säkerhetiseringen av cyberfrågan formats mer kring externa aktörers operationalisering av EU-identifierade hot. (Kommissionen, 2013: s. 3). För att EU som aktör skall kunna säkras finns det två olika sätt. EU som institution och dess medlemsländer. Det råder återigen inget tvivel om att de här två går hand i hand men för att en säkerhetiseringen skall kunna implementeras krävs det att det görs på olika nivåer. EU som säkerhetiseringsaktör är de främsta som driver frågan om något är ett hot och att något/någon är hotad, även om det finns ett flertal olika organisationer och andra interna intressegrupper och aktörer som ligger till grund för besluten. EU:s agerande bygger också på medlemsländernas observationer och nationella bedömningar av hotbilder. Det ger alltså svar på att EU är beroende av att samspelet med medlemsländerna måste nå lukrativa lösningar för att unionen sedan skall kunna bearbeta strategin. Så länge medlemsländerna är oense om lösningar på olika frågor blir även den primära processen innefattad av tröghet, trots att det är EU:s institutioner som innehar platsen som främsta *”säkerhetiseringsaktören”* och därmed ansvar för verkställandet.

I kommissionen uttalande *”Unionens tillstånd. Kommissionen förstärker EU:s svar till cyberattacker.”* (2017) poängterades den återigen slående ökningen av cyberattacker och huvudfokuset riktades mot det kollektiva ansvaret att trappa upp säkerheten för att kunna motverka framtida hotbilder. Med fokus på EU:s operationalisering kring cyberstrategi kändes det här som ett uppvaknande med påvisning om att hela unionen och dess medlemsländer måste agera i större utsträckning tillsammans. I europeiska revisionsrättens briefingdokument *”Utmaningar för en ändamålsenlig EU politik för cybersäkerhet”*(2019)

har hoten identifierats övergripande som sabotageprogram, utpressningstrojaner, DDosattacker, social ingenjörskonst (nätfiske) samt avancerade ihållande hot. Hoten förklarar vilken identifieringen som är primär för att EU skulle kunna motarbeta den stegrande graden av cyberattacker som riktar sig emot varje medlemsland. Genom en grundläggande rekommendation och riskbedömning kunde debatten kring hot och aktörer föras vidare och bringa mer klarhet i vad som saknas i en fullständigt effektiv cyberstrategi och vad medlemsländer bör resonera kring. Det fick sedan svar i kommissionen presenterade strategidokumentet ”Säker 5G-utbyggnad i EU – *Genomförande av EU:s verktygslåda.”* (2020) vilket kom som ett sorts svar på europeiska revisionsrättens presenterade briefingdokument året innan. Den moderniserade problematiken inom cybersfären identifierades mer omfattande genom att varje medlemsland nu genomfört en unik riskbedömning utifrån vilka olika hotbilder och externa IT-aktörer som de upplever. I samband med det öppnade det upp för EU att bearbeta det med ett nytt operationaliseringsupplägg kring hur det skall motverkas. EU hade nu 2020 erhållit en historisk förändring med en större, efterlängtad transparens mot medlemsländerna och genom en samordnad EU-riskbedömning kunde de övergripande hoten identifieras som:

- *Icke-motståndare/oavsiktliga hot.*
- *Enskild hackare*
- *Hacktivistgrupp*
- *Organiserad brottsgrupp.*
- *Infiltratörer.*
- *Statliga aktör eller aktör med statlig inblick.*
- *Cyberterrorister och företagsenheter.*

Jämsides med den numera omfattande identifikationen, och den ökade transparensen gentemot medlemsländerna, hade även *”Genomförandet av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater”* ökat precisionen mot hot vilket resulterat till att EU kunde även identifiera globala aktörer samt exekutivt döma externa stater som begått cyberbrottslighet. I juli 2020 presenterade EU ett dokument över dömda privatpersoner och näringsidkare där Ryssland och Kina (*funktionella aktörer)* stod för främst medverkan till cyberbrottslighet mot unionen. Det var de första

aktörerna som dömdes av EU genom en mer enad röst inom cyberoperationalisering. (Förordning (EU) 2019/796).

Enligt konstruktivismen är aktörernas intresse en faktor som utvecklas ur aktörernas identitet. Inom EU finns eftersträvan om en kollektiv identitet och en förhoppning om att medlemsländerna skall ansluta sig till den identiteten. EU och dess medlemsländer som organisation delar ett flertal grundläggande värderingar och normer, vilket understödjer samarbetet och gör dess funktionen möjlig. Under det senaste decenniet har unionen blivit allt mer sammansatt kring cybersäkerheten eftersom EU har implementerat ett tillvägagångssätt som gjort det möjligt att nå intern transparens, vilket i sin tur har gjort att EU och dess institutioner, med kommissionen i framkant, kunnat agera mer effektivt och önskvärt som en gemensam aktör.

I relation till Buzan m.fl säkerhetsteori kan det tolkas som att EU genomgått en omfattande och behövlig förändring under den här tiden. För att kunna agera som en säkerhetiseringsaktör krävs det en klar identifiering av inte bara hotbilder utan även externa aktörer. Jag upplever att det infunnits en avsaknad av robusta incitament för att kunna agera fullt ut mot identifieringen av de funktionella aktörerna. Sedan kommissionens uttalande om unionens tillstånd 2017 har EU trappat upp cybersäkerheten ännu mer och tillsammans med genomförandet av *förordning (EU) 2019/796* har EU gått emot en cybersäkerhetisering. Cyberproblematiken har genomgått en politiserad process och förflyttat sig till toppen av agendan för att därifrån kunna agera genom nya politiserade åtgärder. En faktor som legat till grund för trögheten kring beslutsfattandet är frågan om hur samarbetet med externa aktörer skall tillfallas, då frågan kring kombination av nyttoprincipen i samband med säkerhetsaspekten övervägts olika. Kaska m.fl (2019) pekade på bekymret kring de externa telekom-jättarna men EU står fortfarande till viss del splittrat i frågan kring hur reglering eller bojkottning av de externa aktörernas IT-infrastruktur skall tillfallas, vilket har problematiserat den kollektiva åtgärdsprocessen som behandlas mer ingående i den specificerade frågeställningen under.

5.3 Insatser och åtgärder

Frågeställning som ligger till grund för den rubriken är:

Vad för insatser och åtgärder har förslagits för att öka säkerheten inom cyberstrategin?

I frågeställningen om identifierade hotbilder och aktörer behandlades åtgärdsprocessen i viss utsträckning, eftersom det krävs åtgärder för att kunna identifiera potentiella hotbilder. Nedan behandlas EU:s insatser och åtgärder mer ingående för att förstå vilka insatser som varit till grund för den utveckling som är ett faktum.

I ”Europeiska unionens råd: ”En europeisk säkerhetsstrategi. *Ett säkert Europa i en bättre värld”* (2009) presenterades en omfattande strategi om EU:s framtidsutsikter och vilka utmaningar som skulle sätta prägeln på det kommande decenniet. IT-säkerheten beskrivs som bearbetad i *”EU:s strategi för ett säkert informationssamhälle”* (2006) men EU-rådet poängterade att IT-brottsligheten hade fått en ny dimension definierat genom ett nytt ekonomiskt, politiskt och militärt vapen. I fråga om åtgärder redogör rådet för:

”Ytterligare arbete krävs på detta område för att undersöka förutsättningarna för en övergripande EU-strategi, öka medvetenheten och förstärka det internationella samarbetet.”(EU-rådet, 2009: s. 13–14).

Den nya dimensionen av cyberhot hade nu tvingat EU att prioritera en framställning och rekonstruktion av en då vag cyberstrategi, med mål att erhålla kapacitet och på ett effektivt sätt kunna motarbeta och förebygger cyberattacker. Åtgärdersönskan här var tydlig från rådet – prioritera arbetet för att framställa en effektiv cyberstrategi. Det här menar Buzan m.fl är en relevant aspekt när det kommer till säkerhetiseringsteorin. För att en process av någonting skall kunna gå emot en säkerhetisering krävs det att närvaron av existentiella hot infinns och extraordinära åtgärder implementeras. Det är där den största skillnaden infinns mellan den mer enkla politiseringsprocessen och säkerhetisering i fråga. Säkerhetiseringens legitimitet grundas i och med att ett hot godkänns av väsentliga aktörer (i det här fallet EU:s institutioner och dess medlemsländer) för att sedan följas upp av ett koncept som poängterar det existentiella hotet mot ett gemensamt objekt (politiserar) och agerar där utefter (säkerhetiserar). (Buzan m.fl 1998: s. 21). EU hade år 2009 identifierat att hotbilden ökat och att nya former av cyberattacker hade blivit ett faktum. På önskan av europeiska rådet presenterade kommissionen ”EU:s strategi för cybersäkerhet: *En öppen, säker och trygg cyberrymd.”* (2013) där åtgärdsprocessen nu hade en mer omfattande grund. Kommissionen poängterade vikten av åtgärder kring att utforma en policy för cyberförsvar och funktioner kopplade till den gemensamma säkerhets- och försvarspolitiken (GSFP), utveckla industriresurser och teknologiska resurser för cybersäkerhet samt upprätta en

sammanhängande internationell policy för cybersäkerhet inom EU och främja EU:s kärnvärden. Det här blev sedan ett faktum då det iscensattes. (Kommissionen 2013: s. 5).

Fyra år efter EU-rådets säkerhetsstrategi yrkade kommissionen i *”Unionens tillstånd. Kommissionen förstärker EU:s svar till cyberattacker.”* (2017) på ett ytterligare samspel då en förhöjd cyberbrottsligheten blivit ett faktum. Syftet nu var att med större handlingskraft implementera nya åtgärder som skulle rikta sig emot att stärka de myndigheter som unionen tillsatt samt få de europeiska länderna att integrera sig mer kring en gemensam EU-identitet. Varningarna om det ökade cyberhotet mot unionen hade nu medfört nya säkerhetsdirektiv, men det var fortfarande en lång väg kvar för att EU skulle kunna vara nöjda. Kommissionen menade att primära åtgärder skulle infatta att stärka resiliens i EU samt att öka handlingskraften och effektiviteten kring avskräckningsverktyg med rot i att straffrättsliga åtgärder skulle fungera som ett skydd. Inte långt efter implementerades den ovan nämnda *”Förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater”* vilket gjorde det möjligt för EU att kunna döma externa aktörer utanför unionen för cyberattacker, och genom en uppryckning sätta en ny prägel på EU som cybersäkerhetsaktör. EU hade sedan 2013 ökat sina resurser, stärkt sin transparens till medlemsländerna och genom europeiska revisionsrättens briefingdokument *”Utmaningar för en ändamålsenlig EU politik för cybersäkerhet”*(2019) poängterades nu den ekonomiska frågan i allt större utsträckning än i tidigare anföranden. Då politisk slagkraft kräver en stark ekonomisk grund uppmanade revisionsrätten till en bättre planering av målsättningar, där finansiering och utgifter skulle leda till primära och effektivare åtgärdsprocesser genom att anpassa investeringsnivåerna till målen. (Revisionsrätten 2019: s. 1). Den transparensönskan som i allt större takt eftersträvats sedan 2009 presenteras även av revisionsrätten genom ett bättre utbyte och samordning av information i form av en ändamålsenlig detektering och hantering. Den tydligaste upptrappningen av åtgärder riktade sig dock emot EU:s budgetutgifter, lämpligare resurser till EU:s byråer samt utbildningsresurser genom att öka kompetensen och medvetenheten. De menade att det krävs en ny form av ekonomisk satsning och planering kring cybersäkerheten för att kunna nå den handlingskraft som tidigare saknats. Genom att investera säkrare, mer och mot rätt incitament skulle EU kunna öka kompetensen, handlingskraften och det interna samarbetet, nu inte bara inom IT-innovationer utan även inom cybersäkerheten. I takt med att cyberattacker expanderat både i kvantitet och i olika former har EU:s strävan efter en mer konsekvent cyberstrategi lett till en säkerhetiseringsfas

som sedan 2017 börjat få färg. Det får ytterligare belägg i kommissionens presenterade strategidokumentet ”Säker 5G-utbyggnad i EU – *Genomförande av EU:s verktygslåda.”* (2020) där åtgärderna nu fått en ytterligare högre standard, samtidigt som de europeiska länderna spelat det säkerhetspolitiska spelet med EU:s institutioner med en större smidighet. Det är en nyckelfaktor. Verktygslådan innefattar ett nytänkande kring åtgärder inom tillämpning av relevanta begränsningar av leverantörer som anses utgöra hög risk – inbegripet uteslutande när så krävs för en effektiv riskreducering. Vilket medlemsländerna själva yrkat på. Stärkta säkerhetskrav för operatörer av mobilnät, undvikandet eller begränsandet av mer omfattande beroenden av en enda leverantör och slutligen en periodisk översyn av de nationella riskbedömningarna parallellt med EU:s riskbedömning. (Kommissionen 2020: s. 5–6).

Buzan m.fl (1998) koncept av säkerhetsteori där den konstruktivistiska synen på gemensamma idéer och värderingar, nu med god handlingskraft, format en rak och effektiv struktur inom EU. De tre senaste åren (2017–2020) har erhållit goda strategiska framsteg inom cybersäkerheten, i relation till det moderniserade nätverket och dess medkomna hotbilder och aktörer. Som presenterat i verktygslådan för 5G (2020) har det implementerats en periodisk översyn av de nationella riskbedömningarna på en nivå som inte tidigare infunnits. Samtidigt har samarbetet kring reglering av externa aktörer fått en modern översyn där begränsning blivit ett faktum, för att kunna säkerhetsställa att EU:s säkerhet ses lika primär som strävan efter att vara världsledande inom informationstekniken. Genom att samordnad en riskbedömning, med acceptans från medlemsländerna att motverka hotbilden, har EU kunnat fullfölja processen mot en säkerhetisering där acceptansen inkluderat de konsekvenser som gör att man vidtar åtgärder som betraktas vara utanför den normala proceduren. Genom ett större fokus på kompetens och utbildning inom området stärktes kunskapen som underlättar för en gemensam syn på problematiken. Därifrån utformas arbetet för att undvika negativa konsekvenser. EU har istället för en tvetolkad och utspridd handlingskraft nu börjat utveckla och forma en miljö där cybersäkerhetens strategi mognat i takt med IT-framgångarna med implementerade målsättningar och åtgärder som fullföljs. Det har varit en tydlig röst från EU den andra halvan av 2010-decenniet. Den konstruktivistiska tanken menar att säkerhet är något socialt konstruerat och att beroende på den specifika aktören upplevs saker varierande. När ett upplevt hot kan få en kollektiv bild genom ny kunskap och kompetens stärks den gemensamma identiteten. När ett enande kring det

specifika hotet sedan följs upp och definieras i den politiska arenan krävs åtgärder och ett möjligt säkerhetiseringförsök uppstår. EU:s åtgärder, med grund i nationella riskbedömningar, har givit en kollektiv hotbild som accepterats, vilket senare fått konsekvenser genom åtgärder. I frågan om säkerhetisering är det en primär viktig aspekt att bedöma för att kunna genomgå processen.

5.4 Diskussion: Cyberstrategins säkerhetiseringsprocess

Analysen av EU:s åtgärder, parallellt med Buzan m.fl säkerhetiseringsteori har visat på att EU genomgått en behövlig förändring inom den här typen av säkerhet. Under det senaste decenniet har avsaknaden av fullständig effektivitet och transparens belysts, men kommit på senare tid att implementerats och visat sig vara användbart. Markopoulou m.fl (2019) poängterade att under 2010-talet har EU haft olika kollektiva utmaningar kring det flexibla samspelet inom cybersäkerhetshantering och det har varit en kausal effekt till politisk tröghet inom beslut och åtgärder. I samband med den senaste verktygslådan 5G (2020) har sådana kausala effekter minimerats genom samordnade riskbedömningar och upplevda hot, som i sin tur öppnat upp för en större smidighet att hantera säkerhetsstrategin i takt med informationsteknikens utveckling. Carrapico och Barrinha (2017) menade att cybersäkerheten ifrågasätter ett antal viktiga dikotomier. Jag vill främst lyfta fram den interna och den civila aspekten. EU har förändrats intern inom den här säkerhetsaspekten och mycket bygger på att problematiken kring cybersäkerheten kommit att ses som ett vardagligt upplevt problem för den civila befolkningen. Ett hot ses inte längre bara som ett hot mot EU, utan i takt med moderniseringen av IT-användning möter individen i det civila samhället dagligen på olika cyberhot. Det har i sin tur banat väg för minskandet av de skillnaderna mellan nationella och europeiska nivåerna när en ideal grund för enhetlighet övervägs inom ett säkerhetsområde. Det är ett signum för att en fråga skall kunna säkerhetiseras, enligt Buzan. Buzan m.fl (1998) menar även att det krävs arbete kring politiska, sociala och ekonomiska mål för att kunna genomföra säkerhetiseringen. Det sociala perspektivet har visat på en acceptans från medlemsländerna i samspel med EU:s institutioner. Det politiska perspektivet inkluderas av de policyförändringar som implementerats och slutligen det ekonomiska perspektivet som har blivit ett faktum av policyförändringar då man anpassat investeringar till de nya primära åtgärderna. EU har identifierat hotbilder och aktörer för att därifrån kunna presentera relevanta åtgärder vilket sågs med en problematik i början av decenniet, med tanke på EU-

rådets uttalande om *”Det ytterligare arbetet som krävs”.* (EU-rådet, 2009: s.13). Köpenhamnsskolan tre nämnda komponenter som kännetecknar en lyckad säkerhetisering inkluderas av existentiella hot, krisåtgärder samt skiftandet av förekommande lagar där den slutgiltiga processen innefattar en lägesändring av samspelet emellan olika grupperingar. Genom säkerhetiseringsteorin har vi således sett ett par starka förändring efter 2017 som innefattas av NIS-direktivet, *”Förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater*” samt kommissionens presenterade strategidokumentet: *”*Säker 5G-utbyggnad i EU – *Genomförande av EU:s verktygslåda.”* (2020). Jämfört med verktygslådan från 2013 infanns nu en större handlingskraft och en större flexibilitet att hantera transparens, uppmana till reglering av externa informationsnätverk och en större definition och slagkraft emot *den funktionella aktören.* Genom mitt empiriska material har de externa hoten presenterats som ett flertal aktörer, där Kina och Ryssland utgjort majoritet. (Förordning (EU) 2019/796). I takt med Kinas önskan att implementera sin informationsteknik världen över genom bland annat telekom-jätten Huawei har EU:s medvetenhet givit nya direktiv. Kaska m.fl (2017) poängterade att potentialen hos 5G-nätverket att bli motorn inom internationell teknik och internetöverföring även format en sårbar implikation inom säkerhetsaspekten. Utifrån EU:s agerande genom ”Säker 5G-utbyggnad i EU – *Genomförande av EU:s verktygslåda.”* (2020) har det tagits i beaktande och säkerheten kring 5G har kombinerat nyttoprincipen mot säkerhetsaspekten i en ny stabiliserad utveckling, för att minimera bakslag av 5G. Åtgärder mot utsatta närverk och nya preciserade riskbedömningar i relation till ett effektivt samspel mellan *referensobjektet* och *säkerhetiseringsaktören* har ökat och det är också en kausal förklaring till varför EU kunnat agera och på ett exekutivt sätt reglera och fördöma vissa *funktionella aktörer,* samtidigt som man implementerat åtgärder för att skydda individen.

Enligt Buzan, Waever och de Wilde är säkerhet som sagt någonting negativt. (Buzan m.fl 1998: s. 29) De menar att möjligheten att hantera olika frågor utan att behöva applicera särskilda förfaranden skall vara möjligt och säkerheten visar på olika aktörers misslyckande att sköta frågor inom den normala politiska sfären. Här har EU förflyttat sig ifrån *den icke-politiserade fasen* (då nätverksmoderniseringen var nyfödd) till *den politiserade fasen* för att slutligen behandla frågan om cybersäkerhet i den mån att *säkerhetiseringsfasen* uppnåtts. För att det här skulle vara möjligt krävdes det av EU att vara medvetna om *referensobjektet, säkerhetiseringsaktören* samt den *funktionella aktören* för att kunna veta hur man skall

operera med största nytta. När en fråga har kommit att bli så pass känslig och äventyrandes av samhällets och individens integritet krävdes det effektiva och flexibla åtgärder som slutligen lett fram till det definitiva steget, säkerhetiseringsfasen. (Buzan m.fl: s. 35–40).

6. Slutsatser

Huvudfrågeställningen: *På vilket sätt har EU:s cyberstrategi säkerhetiserats under perioden 2009–2020?* har lett fram till svaret att EU:s cybersäkerhetsstruktur har förändrats ordentligt mellan de här åren, med stort fokus på perioden 2017–2020. Buzans m.fl teoretiska aspekt kring säkerhetisering innefattar först en intern bild av de figurerande aktörerna som skall identifieras, för att sedan kunna identifiera de externa aktörer och hotbilder, vilket krävs för att sedan nå en acceptans av den politiska agendans problematiseringen och slutligen kunna implementera nödvändiga åtgärder å unionens och medlemsländernas vägnar. Processens av en säkerhetisering är ständigt krävande efter förändring och med rot i att informationstekniken ständigt moderniseras och utvecklas. EU har inte bara förstått utan även börjat operera mer effektivt och flexibelt kring det faktumet. EU:s strävan efter att vara en världsledande aktör inom IT-sfären är stark och kommer förbli det så länge frågan är av högsta grad på den politiska agendan. Om EU kan vara lika framgångsrika inom säkerhetsaspekten kan framtiden erbjuda ännu mer stabilisering och en ännu högre längsta nivå inom unionens säkerhetsstrategi och de cyberattacker som ständigt sker. Vad har vi lärt oss om security teorin? Cyberaspekten är något nytt och EU som säkerhetsaktör har förändrats inom sektorn och gått mot en allt mer säkerhetiseringsaktör, då Buzans kriterier blivit allt mer uppfyllda under det senaste decenniet. Det har även givit väg för att se på säkerhetiseringsteorin ur en annan synvinkel med syfte att förstå att även säkerhetiseringsprocessen har moderniserats och förflyttat sig till andra politiska sakfrågor, som uppfyller de kriterier som Buzan m.fl önskar för en legitim process. När individer i ett samhälle uppfattar en problematik och börjar samtala kring det operationaliseras en *”speech act”* som förflyttar en politisk fråga högre upp på dagordningen. Det krävs alltså inte bara att det politiska etablissemanget uppfattar en problematik, utan även individen i samhället. På så sätt påverkar det säkerhetiseringsprocessen och gör den möjlig för mobilisering.

Koenig-Archibugi (2004) poängterade att de olika medlemsländernas inhemska attityd till den gemensamma utrikes- och säkerhetspolitik som drivs av EU blir en bredtolkad aspekt i flera avseenden då de olika medlemsländernas samverkan kring den kollektiva säkerheten har stark påverkan av den nationella attityden. (Koenig-Archibugi, 2004). Ser man tillbaka på det utifrån dagens läge har mitt resultat visat på att medlemsländerna gått emot en allt mer sammansvetsad och transparent politik inom cybersäkerheten. Det här följer också forskarna

Helena Carrapico och André Barrinha (2017) upp som poängterade vikten av att upprätta en stark samverkan inom unionen och mellan medlemsländerna. Det forskarna har pekat på har blivit ett faktum i takt med att informationstekniken moderniserat och blivit allt mer sårbar för hot. Ijaz Ahmad m.fl (2017) påpekade att säkerhetshotet kommer att vara större än tidigare nätverk och att 5G-nätverket har lett till en kritisk infrastruktur som kräver mer åtgärder för att garantera säkerheten, inte bara den kritiska infrastrukturen utan även för säkerheten i samhället som helhet. Det visade sig också stämma vilket förklaras genom EU:s upptrappning av cybersäkerhetsåtgärder från 2017. EU har strävat efter att bli allt mer sammansvetsat men något som fortfarande ses som en stark utmaning för EU som aktör är de spridda skurarna kring regleringen av den externa IT-infrastrukturen. Samspelet mellan EU:s institutioner, medlemsländerna och andra EU-interna IT-företag har drivit fram olika idéer om vad medlemsländerna och unionen bör göra. De implikationerna, ur ett empiriskt hänseende, kan bidra till en tröghet som Markopoulou m.fl (2019) behandlat och belyser kring EU:s utmaningar för att vara en sammansvetsad och slagkraftig union.

Då cybersäkerhet är ett ytterst aktuellt ämne och min undersökning sträcker sig till nutidens läge öppnar det för vidare forskning på flera områden. Jag tror personligen att området kring riskbedömning och användningen av externa aktörers informationsteknik kommer vara 2020-decenniets största fokus. Eftersom jag förhållit mig till en kvalitativ innehållsanalys skulle en relevant forskningsaspekt vara att göra mer systematiska intervjuer och se hur säkerhetsstrategin fungerar i praktiken. Det är en större deskriptiv skillnad mellan dokument med visioner, mål och åtgärder kontra faktisk operationalisering, därför kan intervjuer av *public opinion* (europeiska folket) och andra intresseaktörer ge en mer djupgående bild. Hur påverkar *”speech act”* säkerhetiseringsprocessen? Och vad ser individerna inom EU för kommande utmaningar inom IT-sfären? Vidare forskning skulle även vara intressant inom de specifika länderna inom unionen gällande extern IT-infrastruktur. Där finns det mycket att undersöka för att förstå och tolka EU:s interna sampel ännu bättre. Nya frågor inom det här området, som inte kunde behandlas i den här studien, landar i hur EU hanterar samspelet med de interna IT-jättarna som till exempel Ericsson, som påverkats av att Huaweis slagkraft i Europa stramas åt för tillfället. Som nämnt ovan krävs det ett samspel mellan EU:s institutioner, medlemsländerna och EU-interna IT-företag för att kunna stimulera säkerhetsaspekten samtidigt som marknaden tar så lite skada som möjligt. IT-världen knyter hela vår globala sfär allt mer samman, men det krävs fortfarande en självständig grund för att

kunna operera utifrån en trygg och stabil lägstanivå. Med det i åtanke är en intressant fråga även att se hur verktygslådan från 2020 följts upp där nya forskningsfrågor inom dess potentiella brister och ytterligare implementering av nya målsättningar och åtgärder kan undersökas, eftersom nätverkets ständiga modernisering även moderniserar hot och cyberattacker. Säkerhetiseringsprocessen är en väldigt komplex politisk procedur, och som nämnt i teorikapitlet - Det är viktigt att tillägga att de tre olika faserna inte är totalt orörliga, det kan ses som problematiskt att veta och påvisa när en fråga blivit säkerhetiserad. Genom att implementera den konstruktivistiska Köpenhamnsskolans teori om säkerhetisering har en förklaring på hur EU:s agerande kring cybersäkerhetsstrategin mellan år 2009–2020 skett. EU:s befann sig i *Den politiserade fasen* år 2004 då IT-myndigheten ENISA föddes och med tidens gång har unionen gått mot en mer säkerhetiseringsprocess där kommissionen uttalande: *”Unionens tillstånd. Kommissionen förstärker EU:s svar till cyberattacker.”* (2017) är ett avstamp gällande en ny riktning för EU och dess säkerhetspolitik. Undersökningens syfte har visat att det kommer krävas uppoffringar om en konsekvent säkerhetspolitik i relation till nätverksmodernisering skall kunna upprätthållas och värna den europeiska säkerheten.

Referenslista

Bergström, G. & Boréus, K. (Ed.). (2012). Textens mening och makt: metodbok i samhällsvetenskaplig text- och diskursanalys. (3., [utök.] uppl.). Studentlitteratur. ISBN: 978-91-44-07476-4

Buzan, Barry – Waever, Ole – de Wilde, Jaap, (1998). Security – A New Framework for Analysis. London: Lynne Rienner. ISBN: 978-1-55587-603-6

Dimitra Markopoulou, Vagelis Papakonstantinoua, Paul de Hert. (2019). The new EU cybersecurity framework*: The NIS Directive, ENISA's role and the General Data Protection Regulation.* Computer Law & Security Review. Volume 35. 105336

Gerrard Quille. (2004). The European Security Strategy: *A Framework for EU Security Interests?* International Peacekeeping, Vol.11, No.3. ISSN 1353-3312.

Helena Carrapico, André Barrinha. (2017). *The EU as a Coherent (Cyber)Security Actor?*

Ijaz Ahmad, Madhusanka Liyanage, Tanesh Kumor, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov (2017). 5G Security: *Analysis of the thretas and solutions.*

J. Scott Marcus, Marieke Klaver. (2011). *The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally.*

Justesen, L. & Mik-Meyer, N. (2011) Kvalitativa metoder: *Från vetenskapsteori till praktik.* Studentlitteratur. ISBN: 978-91-44-07546-4

Kadri Kaska, Henrik Beckvard and Tomáš Minárik. (2019). *Huawei, 5G and China as a Security Threat.*

Mathias Koenig-Archibugi. (2004). *Explaining government preferences for institutional change in EU foreign and security policy*.

Reus-Smit, Christian, (2009). "Constructivism". I: *Theories of International Relations*, Burchill, Scott – Linklater, Andrew (red.) New York: Palgrave Macmillan. Fourth Ed. pp. 212-236. ISBN: 978-0-23021-923-6

Sheehan, Michael, (2005). *International Security – An Analytical Survey*. London: Lynne Rienner Publishers. ISBN: 978-1-62637-938-1

Soltani, Fakhreddin, Jayum A. Jawan, Ahmad, Zaid. B (2014). *Constructivism, Christian Reus-Smit and the Moral Purpose of the State*

Bilagor

ALLEA. All European Academies (2017). *Den europeiska kodexen för forskningens integritet.* https://www.vr.se/download/18.7f26360d16642e3af99e94/1540219023679/SW_ALLEA_Den_europeiska_kodexen_f%C3%B6r_forskningens_integritet_digital_FINAL.pdf (Hämtad 2021-02-17).

ENISA. (2004). About ENISA - The European Union Agency for Cybersecurity. *Towards a Trusted and Cyber Secure Europe.* https://www.enisa.europa.eu/about-enisa (Hämtad 2021-01-05).

Europeiska revisionsrätten**.** (2019 – mars). *Utmaningar för en ändamålsenlig EU politik för cybersäkerhet.* Briefingdokument. (Hämtad 2021-01-05).

Europeiska unionen. Utrikes- och säkerhetspolitik. EU:s utrikes- och säkerhetspolitik https://europa.eu/european-union/topics/foreign-security-policy_sv#:~:text=EU%3As%20utrikes%2D%20och%20s%C3%A4kerhetspolitik,av%20EU%3As%20internationella%20arbete (Hämtad 2021-01-05).

Europeiska unionens råd. (2009). En europeisk säkerhetsstrategi: *Ett säkert Europa i en bättre värld.* (Hämtad 2021-01-05).

Förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater **-** https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN (Hämtad 2021-01-05).

Gemensamt meddelande från kommissionen till europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén. (2013 – 7:e februari). EU:s strategi för cybersäkerhet: *En öppen, säker och trygg cyberrymd.* (Hämtad 2021-01-05).

Lindstedt, Urban (2010). Internet dödade kalla kriget. https://www.jajja.com/jajja-magazine/internet-dodade-kalla-kriget/ (Hämtad 2021-03-08).

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska Ekonomiska och Sociala kommittén samt regionkommittén. (2020 – 29:e januari*).* Säker 5G-utbyggnad i EU – *Genomförande av EU:s verktygslåda.* (Hämtad 2021-01-05).

Redaktionen för EU-upplysning. Myndigheten för samhällsskydd och beredskap (MSB). https://www.msb.se/sv/publikationer/international-case-report-on-cyber-security-incidents--reflections-on-three-cyber-incidents-in-the-netherlands-germany-and-sweden/ (Hämtad 2021-01-05).

Unionens tillstånd (2017 – 19 september). Cybersäkerhet: *Kommissionen förstärker EU:s svar till cyberattacker.* (Hämtad 2021-01-05).