NORDISKT SAMARBETE FÖR PSYKOLOGISKT FÖRSVAR

10 FÖRSLAG FÖR ÖKAD MOTSTÅNDSKRAFT

SAMMANFATTNING

Omvärldsläget aktualiserar behovet av att öka kunskapen om hur de nordiska länderna enskilt och tillsammans kan upptäcka, förstå och möta påverkansoperationer. Det senaste året har tydliggjort att hybridhot (exempelvis ekonomiska påtryckningar, cyberangrepp och desinformation) har blivit mer sofistikerade, och att främmande makt och andra antagonister utnyttjar samhällets sårbarheter för att illegitimt nå sina politiska och ekonomiska målsättningar.

Även om EU och Nato är de nordiska ländernas starkaste säkerhetspolitiska samarbeten i ett europeiskt och transatlantiskt perspektiv, så finns det ett stort värde i att utveckla det regionala nordiska samarbetet. För förståelse och innovation – för stärkt motståndskraft.

Handling och beslut av den politiska nivån är avgörande för att vi ska stärka våra länders strategiska respektive operativa förmågor att identifiera och möta påverkansoperationer och desinformation.

HUVUDPUNKTER

- Utvecklingen vad det gäller spridningen av desinformation och möjligheterna till att manipulera innehåll i exempelvis sociala medier är stor. Idag finns det en global industri när det kommer till varor och tjänster för ogrundad information.
- Det har blivit väldigt tydligt hur kriser så som coronapandemin exponerar våra kognitiva sårbarheter, det vill säga svårigheter att förstå till exempel sammanhang eller orsak och verkan. Dessa utnyttjas av antagonister för framgångsrik påverkan.
- Vi behöver öka vår förståelse för hur olika händelser och aktiviteter i den digitala miljön påverkar oss. Det för att upprätthålla och skydda vår **digitala suveränitet** och **kognitiva suveränitet**, i samma omfattning som vi upprätthåller och skyddar vår territoriella (luft, land, hav) suveränitet.
- Påverkansoperationer sker oftast inte över dagar eller veckor. Vanligast är att det genomförs med ett långt tidsperspektiv på ett lågintensivt sätt, så att vi inte ens märker att det sker. Därför är det proaktiva arbetet fundamentalt, ett modernt psykologiskt försvar är något som samhället måste bedriva brett och kontinuerligt.
- Med avstamp i nationella solidaritetsförklaringar och etablerade nordiska samarbeten såsom Nordefco, Nordiska ministerrådet och Haga-deklarationen finns det stora vinster med att utveckla samverkan, samordning och samarbete inom området psykologiskt försvar.

Definitioner

Följande definitioner och begrepp används i detta *fagnotat*. Då texten vänder sig till läsare i alla de nordiska länderna så är definitionerna på engelska, det för att minska risken att de feltolkas.

Desinformation (Disinformation)
The creation, presentation, and dissemination of “verifiably false content” for “economic gain or to intentionally deceive the public and may cause public harm.”

Hybridhot (Hybrid Threats)
A threat of mixed origin that avoids declaration of war and accountability.

Informationsmiljön (The Information Environment)
Dynamic physical and/or virtual settings interpreted by the mind.

Missinformation (Misinformation)
The distribution of verifiably false content without an intent to mislead or cause harm.

Narrativ (Narrative)
Morals drawn from stories.

Påverkansoperationer (Influence Operations)
Coordinated efforts to influence a target audience using a range of illegitimate and deceptive means, in support of the objectives of an adversary.

Strategisk kommunikation (Strategic Communication)
A holistic approach to communication based on values and interests that encompasses everything an actor does to achieve objectives in a contested environment.

Påverkansoperationer: En lägesbild

Det senaste året har tydliggjort att hybridhot (exempelvis ekonomiska påtryckningar, cyberangrepp och desinformation) blivit mer sofistikerade. Här ges några exempel på händelser och trender inom området påverkansoperationer och desinformation.

Den pågående infodemin

Desinformation dödar – det senaste året har tusentals människor runt om i världen blivit svårt sjuka och många har dött till följd av att de trott att covid-19 är en bluff, eller för att de självmedicinerat med exempelvis metanol.[1] Hundratals telemaster har saboterats och telekompersonal trakasserats för att konspirationer om 5G-utbyggnaden kopplas ihop med spridningen av covid-19. Efterhand har narrativen kommit att handla alltmer om covid-19-vaccin. Flertalet aktörer bidrar aktivt till att skapa oro och sprida vilseledande information. Budskap från anti-vaxers och konspirationsteoretiker utnyttjas och förstärks av statsaktörer, liksom ekonomiska bedragare och populistiska alternativmedier.[2, 3]

Sedan coronapandemins utbrott i början av 2020 så pågår en infodemi, en global informations-pandemi.

> *"...the greatest strength of our societies – an open, robust public debate – now risks being its greatest vulnerability. Unconstrained by the requirements of honesty, truth or self- respect, attackers can use our information system to confuse us and disrupt our public life."*
>
> — **James Pamment [4]**

Konsekvenserna har varit allvarliga och det senaste året har det blivit uppenbart hur desinformation är ett betydande hot mot vår välfärd, mot våra demokratiska samhällen.

Det har blivit väldigt tydligt hur kriser så som **denna pandemi exponerar våra kognitiva sårbarheter**, det vill säga svårigheter att förstå till exempel sammanhang eller orsak och verkan. Dessa utnyttjas av antagonister för framgångsrik påverkan.

Angrepp mot demokratin

Sedan den ryska inblandningen i det amerikanska presidentvalet 2016 så har påverkansoperationer och desinformation uppmärksammats alltmer som hot mot demokratin. De senaste åren har ett stort antal nationella val utsatts för försök till illegitim påverkan, av olika omfattning och intensitet. Atlantic Council lanserade inför det amerikanska presidentvalet förra året *Interference 2020* – ett verktyg som gav en tydlig bild av hur omfattande främmande makters påverkan med koppling till val är idag. I en rapport från Oxford Internet Institute[5] beskriver forskarna att de funnit bevis på att 81 länder under år 2020 har använt sig av sociala medier för att sprida politisk propaganda och desinformation.

Ett växande problem är hat och hot mot enskilda individer, där exempelvis politiker, journalister och forskare utsätts för trakasserier och direkta hot.[6, 7, 8] Denna utveckling medför bland annat en ökad risk till självcensur vilket är ett allvarligt problem. Dessa yrkesgrupper som har stor betydelse för det demokratiska samtalet måste våga genomföra sitt arbete fullt ut.

Idag finns det en global industri

Att värja sig mot påverkansoperationer 2021 är något helt annat än vad det var för några år sedan. Den ryska påverkanskampanjen 2016 mot det amerikanska presidentvalet genomfördes i huvudsak av en trollfabrik och ett par statsunderstödda enheter för cyberangrepp. Idag kan exempelvis en kinesisk statsaktör köpa en påverkanskampanj av ett tyskt företag med ryska, ghanesiska och filippinska underleverantörer – och rikta denna kampanj mot amerikanska målgrupper.[9]

Utvecklingen vad det gäller spridningen av desinformation och möjligheterna till att manipulera innehåll i exempelvis sociala medier är stor. Idag finns det en global industri när det kommer till varor och tjänster för ogrundad information. Infrastrukturen för utveckling och underhåll av manipulerings-programvara för sociala medier, generering av fiktiva konton och att tillhandahålla mobila proxyservrar växer. I stor utsträckning annonseras och säljs dessa tjänster och varor i öppna kanaler.[10] Liksom aktörer som arbetar med laglig sälj och marknadsföring så kan illegitima aktörer köpa data om de olika målgrupper man vill påverka av Data Brokers (företag som samlar in och sammanställer information om privatpersoner och säljer informationen vidare till andra företag). Idag finns runt 5 000 globala Data Brokers, vars samlade intäkter uppgår till 178 miljarder dollar. Denna marknad är svår att överblicka och gränslinjerna mellan vad som är legitim, illegitim och illegal verksamhet är otroligt svåra att avgöra.[11, 12]

"Follow the Money"

Det vedertagna begreppet "follow the money", som syftar på att om man vill lösa brottet ska man följa pengarna, är verkligen relevant när det kommer till att identifiera och möta desinformation. Ett problem är att stora välkända varumärken oavsiktligt betalar enorma summor för reklam på "desinformationssidor". Enligt organisationen Global Disinformation Index bedömning så tjänade europeiska "desinformationssidor" sammanlagt runt 76 miljoner dollar under 2020 på annonser på sina sidor.[13]

När forskare har analyserat hur antivaccinations-hemsidor tjänar stora summor på annonser så har de identifierat att många av dessa sidor lyckats kringgå plattformarnas åtgärder för att stoppa missinformation och desinformation kopplat till covid-19. Det genom att installera och konfigurera olika kombinationer av mjukvara.[14] **Att begränsa möjligheterna till finansiering av desinformation skulle ha stor effekt på dess omfattning och spridning.**

Manipulerade data för kognitiv påverkan

Idag är det relativt enkelt att producera sofistikerad desinformation, exempelvis "deepfakes". Med hjälp av artificiell intelligens/maskininlärning manipuleras video, text och röst. Manipulerat innehåll som kan användas till exempelvis ekonomiska bedrägerier[15] eller för att underminera förtroende för en person eller tjänst. Ett annat hot är manipulering av positions eller metadata i syfte att påverka våra attityder och beteenden. Exempelvis har det spridits falsk information på sjöfartstjänster som *MarineTraffic* om hur svenska marinens fartyg rör sig på haven – att svenska fartyg kört nära den ryska enklaven Kaliningrad.[16]

Vad är psykologiskt försvar

Psykologiskt försvar är ett svårfångat begrepp och i Norden så är det egentligen bara i Sverige som begreppet används.

En svensk definition är: **Det psykologiska försvarets ändamål är att värna det öppna och demokratiska samhället, den fria åsiktsbildningen samt Sveriges frihet och oberoende**. Finland använder ett närliggande begrepp: "Mental kristålighet".

Utifrån den svenska Psykförsvarsutredningen[17] så är det i stort följande som ska försvaras:

> *"I det moderna informationssamhället blir det allt svårare att särskilja vem som är vad, och vad som är en fullt legitim åsiktsbildning i en demokrati och vad som är delvis manipulerat utifrån."*
>
> — **Patrik Oksanen**[18]

- Nationens oberoende och självständighet
- Demokratin och den fria åsikts- och opinionsbildningen
- Förtroende och tillit, dels människor emellan, dels till den offentliga förvaltningen

Utifrån dessa skyddsvärden ska det psykologiska försvaret skydda mot:

- Valpåverkan
- Hot och ryktesspridning riktat mot politiker, tjänstemän, forskare, journalister m.fl.
- Desinformation riktad mot samhällets grundläggande funktionalitet
- Informationspåverkan som en förberedelse för eller som ett led i ett väpnat angrepp

I rapporten *Defence against foreign influence* från Forsvarets forskningsinstitutt[19] angrips området psykologiskt försvar utifrån ett värdebaserat synsätt. Rapporten bygger på dessa tre områden:

- Definiera vad skada är
- Värdera vad främmande makts påverkan skadar
- Beskriv syftet med motåtgärder

Utifrån dessa områden rekommenderas staten göra en översikt över dess väsentliga säkerhetsintressen. Att det som staten värderar mest är också det viktigaste att skydda. Finlands skrift *Säkerhetsstrategin för samhället, Statsrådets principbeslut*[20] är ett tydligt exempel på hur det skulle kunna se ut – på vad en stat värderar mest. I den finska strategin kategoriseras de statliga säkerhetsintressen i sju "vitala funktioner":

- Ledning
- Internationell och EU-verksamhet
- Försvarsförmåga
- Den inre säkerheten
- Ekonomi, infrastruktur och försörjningsberedskap
- Befolkningens handlingsförmåga och service
- "Mental kristålighet"

Vi behöver förstå informationsmiljön

För att förstå hur väl förberedda vi är och hur vi ska skydda oss mot påverkansoperationer och desinformation – så måste vi förstå informationsmiljön. Informationsmiljön används ofta som en beskrivning av det moderna medielandskapet med traditionella och sociala medier. Men informationsmiljön som begrepp och modell har ett större användningsområde. I *Hybrid Threats: A Strategic Communications Perspective*[21] från StratCom COE används informationsmiljön som en modell för att förstå hur olika händelser och aktiviteter påverkar oss. Hur olika aktörer och målgrupper interagerar, hur människor ser på omvärlden, och vad som i slutändan påverkar deras beslut.

Informationsmiljön består av tre dimensioner, den *kognitiva*, den *fysiska* och den *digitala*. Dessa tre hänger samman och de påverkar varandra. Exempelvis att ett fysiskt angrepp framför allt kan syfta till att påverka oss kognitivt, en symbolhandling som genomförs för att uppnå ett politisk mål. Eller så kan spridningen av ett narrativ i digitala kanaler syfta till att påverka individer och grupperingar att genomföra sabotage. Ett tydligt exempel i närtid är vilseledande och felaktig information kring att etableringen av 5G-teknik bidrar till spridningen av covid-19. Förståelse och analys av olika komponenter i informationsmiljön kan hjälpa oss att förstå hur hybridhot utnyttjar sårbarheter i samhället. För att möta hybridhot är det därför fundamentalt att ta itu och lösa inhemska problem och utmaningar som sårbarheter i tekniska system, liksom sociala klyftor och politikerförakt. **Den enskilda individen är alltid den mest sårbara och lättast åtkomliga länken.**

De nordiska länderna och psykologiskt försvar

Mellan de nordiska länderna finns det både likheter och olikheter när det kommer till psykologiskt försvar (en översikt finns i *En ny myndighet för att stärka det psykologiska försvaret*). Gemensamt är att regeringarna genom utrikes-, försvars- och justitiedepartement, liksom myndigheter och organisationer som är verksamma inom områdena samhällsskydd, försvar, säkerhets- och underrättelsetjänst, och media har ett stort ansvar. Nedan uppmärksammas några exempel från Danmark, Finland, Norge och Sverige.

Danmark
Under senare år har Danmarks arbete mot desinformation och påverkansoperationer intensifieras. Exempelvis presenterade regeringen 2018 en handlingsplan med 11 punkter för att motverka hotet om utländsk påverkan vid val. Bland de 11 punkterna fanns bland annat:

- En tvärministeriell ”task force” för att stärka koordineringen av myndigheternas insatser i samband med val.
- Ett uppdrag till utrikesdepartementet gällande förstärkt övervakning av desinformation i media riktat mot Danmark. I uppdraget ingår även stöd till ambassader, medier och allmänhet.[22]

I den utrikes- och säkerhetspolitiska strategin för 2019–2020 så fanns en inriktning om att stärka insatserna mot utländska påverkanskampanjer som ”hotar danska värderingar och intressen”.[23]

Finland
Finland har i *Säkerhetsstrategin för samhället, Statsrådets principbeslut* definierat mental kristålighet som ”individers, sammanslutningars och samhällets samt nationens förmåga att utstå den mentala press som krissituationer orsakar och klara av effekterna av den. God mental kristålighet underlättar återhämtningen efter kriser”. I den nationella säkerhetsstrategin framhålls att den mentala kriståligheten ”har ökat i betydelse som fundament för samhällets säkerhet”.[24] Finland har kommit långt i arbetet med psykologiskt försvar. Exempelvis inrättade de ett separat utbildningssystem redan 2014 för skolelever, journalister och andra prioriterade målgrupper för att öka kompetensen inom desinformation och källkritik.

Norge
Hotet från påverkansoperationer och desinformation upplevs fått mindre uppmärksamhet i Norge än i de nordiska grannländerna under 2010-talet. Men har ökat under de senaste åren, särskilt kopplat till valpåverkan. Exempelvis tog regeringen fram en handlingsplan som syftade till att stärka motståndskraften mot hybridhot och påverkansoperationer i samband med 2019 års kommunestyre- och fylketingsvalg.[25] Och i regeringens melding *Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden*[26] presenteras bland annat följande politiska förslag för att öka motståndskraften mot hybridhot så som desinformation:

- Vidareutveckla förmågan att etablera,

upprätthålla och analysera en sektorövergripande lägesbild på strategisk nivå för civilsamhället.
- Värdera och utveckla möjligheterna till att lägga samman civila och militära lägesbilder för en bättre nationell helhetsbild.
- Vidareutveckla samarbetet mellan justitie- och beredskapsdepartementet och försvarsdepartementet avseende informationsdelning kring hotbilder, hotaktörer och sårbarhetsanalyser.
- Stärka skolelevers förmåga till källkritik genom introduktionen av den nya läroplanen (*Kunnskapsløftet 2020*).

Norge har sedan en tid upprättat en tvärsektoriell ”task group”, *Depstrat*, men den är endast operativ när ett departement begär stöd. Gruppen leds av försvarsdepartementet med deltagare från bland annat statsministerns kansli, justitie- och beredskapsdepartementet, e-tjänsten, polisens säkerhetstjänst, Forsvarets forskningsinstitutt och Forsvarets mediesenter.

Sverige
I Sverige så ska en ny myndighet för psykologiskt försvar inrättas, den ska vara på plats i januari 2022. Uppgifterna för myndighet blir bland annat att:

- Identifiera, analysera, och kunna lämna stöd i bemötandet av otillbörlig informationspåverkan och annan vilseledande information som riktas mot Sverige eller svenska intressen.
- Bedriva utbildning och övningsverksamhet inom myndighetens ansvarsområde.
- Verka för samverkan mellan myndigheter och övriga aktörer i det förebyggande arbetet, samt skapa förutsättningar för och bidra till att säkerställa ett samordnat operativt agerande.

Exempel på europeiska och nordiska samarbeten

Europeiska kommissionen bedriver ett arbete för att etablera ett EU gemensamt ramverk för att motverka hybridhot. I enkelhet så styrs det av kommissionens meddelande till parlamentet och rådet från 2016, *Gemsamsam ram för att motverka hybridhot*,[27] och därefter rådets slutsatser om *förstärkt skydd mot hybridhot*.[28] Ytterligare beskrivning finns i en skrift från rådets arbetsgrupp med hybridfrågor.[29] Hanteringen av hybridhot är prioriterad i kommissionens strategiska agenda för 2019–2024.[30] Exempel på projekt som stödjer detta är *European Democracy Action Plan (EDAP)*[31] som har ett område som specifikt handlar om att möta desinformation. Dessutom så driver Europeiska kommissionen ett strategi- och policyarbete under rubriken “A Europe fit for the digital age” som syftar till att öka EU:s digitala suveränitet och utveckla gemensamma europeiska standarder. I december 2020 publicerade kommissionen ett nytt regleringsförslag: *Digital Services Act (DSA)*. Förslagets övergripande syfte är att bidra till en bättre miljö för det demokratiska samtalet i en digital tid. Det genom att skapa en bättre översyn och transparens kring sociala medier och att reducera systematiska risker såsom manipulation och desinformation.[32] Även om Norge inte är med i EU så är Norge bundet till att följa alla rättsakter avseende den inre marknaden och Norge har även svarat kommissionen att de stödjer aktuellt förslag[33] (Norge följer redan idag “e-Commerce Directive”, GDPR, osv).

Det finns idag flertalet överenskommelser och samarbeten på europeisk nivå kopplat till hybridhot och påverkansoperationer. Exempelvis finns kunskapscentret för att möta hybridhot, Hybrid COE i Helsingfors. Där Danmark, Finland, Norge och Sverige är medlemmar. Vid Natos kunskapscenter för strategisk kommunikation, StratCom COE i Riga, är Danmark, Finland och Sverige, men inte Norge representerade. Det gäller även för EU:s utrikestjänst EEAS och *East StratCom Task Force*.[34] En enhet som framför allt fokuserar på pro-ryska narrativ riktade mot EU och dess medlemsländer (*EUvsDISINFO* är en del av detta). Ett annat relevant samarbete är Multinational Capability Development Campaign (MCDC)[35] där Danmark, Finland och Norge medverkat inom *Countering Hybrid Warfare Project*. Ett projekt där Norge varit en ledande nation och vars arbete blivit tongivande för försvarsmakter i hela regionen.

På politisk nivå så finns det inget samarbete på nordisk nivå av samma dignitet som det inom EU, även om Nordiska rådet har genomfört en hel del aktiviteter de senaste åren. Exempelvis så hade Toppmötet 2018 en punkt på temat ”Demokratin under press”[36] och under 2018 släpptes även en gemensam rapport *Fighting Fakes – The Nordic Way*.[37] 2018 publicerade även Myndigheten för samhällsskydd och beredskap (MSB i Sverige) rapporten *Så bygger vi säkerhet i Norden*,[38] och förra året skulle det genomförts temasession ”Desinformation som ett hot mot den nordiska modellen”, men den blev inställd på grund av pandemin.[39] Sverige och Finland har haft bilateral övningsverksamhet där tjänstemän från de båda länderna deltagit.[40] Finska myndigheter har även

anpassat den svenska handboken *Att möta informationspåverkan* (MSB)[41] till sin nationella kontext.

Under hösten 2020 genomförde Nordicom (Nordiska rådet) och Statens Medieråd (Sverige) en serie webinar som behandlade medie- och informationskunnighet i de nordiska länderna.[42] Nordicom är även med och finansierar NordMedia Network som är ett nordiskt nätverk för media- och kommunikationsforskning, vilka exempelvis arrangerar konferensen *NordMedia2021 Crisis and Resilience: Nordic Media Research on the Frontline*.[43] Ett annat akademiska samarbete är *NORDIS – network on online disinformation.* Ett gemensamt projekt med forskare och akademiker från norska, svenska och danska universitet. Där bland annat tre större konferenser/workshops har arrangerats under 2019–2021.[44]

Proaktivt arbete för ökad motståndskraft

Som nämns ovan sker påverkansoperationer oftast inte över dagar eller veckor, utan oftast genomförs de med ett långt tidsperspektiv på ett lågintensivt sätt, så att vi inte ens märker att de sker. Därför är det proaktiva arbetet fundamentalt, ett modernt psykologiskt försvar är något som samhället måste bedriva brett och kontinuerligt. Psykologiskt försvar är en uppgift för samtliga nationella myndigheter.[45]

Det finns förutsättningar för att ett ökat nordiskt samarbete skulle bidra till att öka vår samlade förmåga att identifiera och möta påverkansoperationer. I år när exempelvis **Norge har tillsatt en ny försvarskommission och Sverige arbetar med att ta fram en ny nationell säkerhetsstrategi så finns ett momentum när det kommer till att utveckla det nordiska samarbetet inom krisberedskap och civilt försvar**. Dessa instanser bör undersöka och värdera hur olika nordiska samarbeten kan utvecklas i syfte att öka vår samlande motståndskraft mot hybridhot så som desinformation.

Det samma gäller de nordiska ländernas pågående arbete med att utvärdera den egna hanteringen av cornapandemin. Hur kan olika samarbeten mellan de nordiska länderna utvecklas för att vi i framtiden ska vara bättre förbereda för att hantera en pandemi liksom en infodemi. **Det går att stänga fysiska gränser, men desinformation tar inte hänsyn till det**. Utan den digitala respektive kognitiva dimensionen är och förblir öppen.

I de nordiska länderna behövs det ett ökat engagemang på politisk nivå

Även om EU och Nato är de nordiska ländernas starkaste säkerhetspolitiska samarbeten i ett europeiskt och transatlantiskt perspektiv, så finns det ett stort värde i att utveckla regionala samarbeten. Exempelvis ett starkare nordiskt samarbete när det kommer till hanteringen av den säkerhetspolitiska utvecklingen i norr och Arktis, och ett utvecklat samarbete mellan Norden och de baltiska staterna, NB8, när det kommer till Östersjön. Med avstamp i nationella solidaritetsförklaringar och etablerade samarbeten, såsom Nordefco, Nordiska ministerrådet och Haga-deklarationen, går det att förstärka och utöka det nordiska samarbetet för att bygga förmåga till motståndskraft och motåtgärder mot hybridhot så som desinformation. **Med ett distinktare samarbete på politisk/strategisk nivå så skapas bättre förutsättningar till samverkan och samarbete även på operativ och taktisk nivå.**

Det finns många goda exempel på etablerad samverkan och samarbeten mellan myndigheter, akademi, näringsliv och ideella organisationer i de nordiska länderna att bygga vidare på. Och på politisk nivå så har exempelvis Nordiska rådet i början av 2021 lyft att de vill se ett utökat samarbete när det kommer till utrikes- och säkerhetspolitik. Liksom att de nordiska länderna har mycket att vinna på att stärka sitt samarbete kopplat till krisberedskap och civilt försvar.[46, 47]

2019 fastställdes *En gemensam strategi för samhällssäkerhet*[48] där det framkommer att de nordiska länderna ska utveckla samarbetet för att möta hybridhot, och förra året kom rapporten *Nordic Foreign and Security Policy 2020*.[49] I rapporten presenterades 14 förslag för hur det nordiska samarbetet kan utvecklas. Ett av dem är att utveckla en gemensam, konceptuell och politisk förståelse för hybridhot. **Men det krävs ett ökat engagemang för att bygga faktisk förmåga, och frågor som cyberangrepp och desinformation måste generera mer politiskt kapital.**

10 förslag för ökad motståndskraft

Även om expertisen inom många organisationer är omfattande så är fortsatt de "samarbeten" som finns på en förhållandevis basal nivå. **Det behöver förändras.** Det finns flera områden där de nordiska länderna kan utveckla befintliga, och etablera nya, former av samverkan, samordning och samarbete. I syfte att bygga gemensam förmåga till motståndskraft och motåtgärder mot påverkansoperationer och desinformation.

1. Ny karta – nytt läge

Sociala medier är idag en del av den offentliga infrastrukturen. En utveckling som medfört fantastiska möjligheter, men också stora utmaningar. Trots att det är över 15 år sedan Facebook grundades så ser det nu ut som att politiker, såväl som techbolagen själva, yrvaket försöker hantera en situation som ingen riktigt kunnat förutse. Få aktörer, om ens någon, har riktigt koll på läget. Med utgångspunkt i informationsmiljön som modell så behövs det ett större fokus på:

- Vad digitaliseringen innebär för **de viktigaste av våra skyddsvärden**: liv och hälsa, människors fri- och rättigheter, demokrati, och samhällets funktionalitet.
- **Det demokratiska samtalet** i en digital tid där cybersäkerhet och påverkansoperationer och kunskapsresistens är stora utmaningar.
- Att upprätthålla och skydda vår **digitala suveränitet** och vår **kognitiva suveränitet** liksom vi upprätthåller och skyddar vår territoriella (luft, land, hav) suveränitet.

2. Quadruple Helix

För att öka medvetenheten och bygga motståndskraft kan **samverkan mellan olika aktörer och sektorer** bidra. Samverkan mellan offentlig sektor, universitet/högskola och näringsliv kallas *Triple Helix-modellen*. När civilsamhällets tongivande individer, entreprenörer, startups, ideella organisationer och eldsjälar – grupper med en avgörande roll för innovation och utveckling – kompletterar de traditionella aktörerna skapas en *Quadruple Helix*. Centrala aktörer behöver skapa incitament och forum för samverkan enligt denna modell på olika nivåer, både nationellt och över landsgränserna för att:

- Etablera en gemensam förståelse för hur våra sårbarheter utnyttjas av antagonister för effektiv påverkan.
- Etablera och utveckla metoder för hur vi kan omsätta och implementera all den kunskap som finns till faktiska förmågor.
- Näringslivet ska bli mer medvetna, men också hitta samarbetsformer och metoder där näringslivet kan bli mer transparant utan att det skadar varumärken, samtidigt som de kan bidra och få stöd mot cyberangrepp och påverkansoperationer.

- Skapa förutsättningar för effektivare samverkan och samarbete mellan näringslivet och den akademiska världen. Båda dessa gruppers färdigheter och kunskaper är avgörande för att etablera effektiva metoder och verktyg för att möta påverkansoperationer.

3. Identifiera roller och skapa synergier

Ett aktivt föregångsskap genom politiska beslut och regleringar är centralt för utveckling av ett modernt psykologiskt försvar. Men det är också oerhört viktigt att **uppmuntra och på olika sätt stimulera goda initiativ**, små som stora, som bidra till psykologiskt försvar:

- Identifiera roller och ansvar, kartlägg vilka aktörer och förmågor som finns i de olika länderna med verksamhet som bidrar till psykologiskt försvar.
- Ta fram planer för hur synergier kan uppstå och förstärkas mellan olika verksamheter.

4. Nordisk fact-checking

Eftersom desinformation och missinformation inte tar hänsyn till landsgränser så skulle ett utvecklat samarbete avseende identifiering och debunking minska spridningen och effekterna av felaktig och vilseledande information (exempelvis så granskar den norska organisationen Faktisk ofta felaktig information om Sverige som sprids i norska forum):

- Skapa incitament och bidra till att **utveckla samverkan och samarbeten mellan de nordiska organisationer som arbetar med fact-checking**.

5. Involvera forskningen

Den forskning som sker vid nationella centrum, myndigheter och universitet, liksom internationella organisationer och samarbeten såsom StratCom COE och MCDC, påvisar att de nordiska länderna många gånger har tillgång till den absoluta expertisen inom aktuella områden. Ett arbete som kan utvecklas är att **enskilt och tillsammans omsätta all denna kunskap till nationella och nordiska förmågor – strategiska såväl som operativa**. Det finns stora vinster med tätare samarbete mellan politiken och akademin. Involvera akademiker och experter i det politiska arbetet och för att realisera teoretiska kunskaper och bygga faktisk förmåga. Två tydliga exempel att inspireras av är:

- Utvecklingen av brittiska *RESIST Counter Disinformation Toolkit*. Utifrån den svenska handboken *Att möta informationspåverkan* är *RESIST* en vidareutveckling. Där forskarna vid Lunds universitet tillsammans med Government Communication Service (GCS) utvecklat en verktygslåda för att förebygga och hantera spridningen av desinformation. En väldigt konkret såväl som allomfattande verktygslåda för kommunikatörer såväl som policy-skapare, chefer och seniora rådgivare.
- Utvecklingen av *Global Britain in a competitive age*. Akademiker från School of Security Studies vid King's College London, har haft nyckelroller i framtagandet av den nyligen publicerade nya nationella säkerhetsstrategin.[50]

6. En gemensam terminologi

Det är nödvändigt att tydligare definiera och inrikta psykologiskt försvar liksom att **etablera en gemensam terminologi på nationell nivå. Än bättre på nordisk nivå.** För idag finns det en stor spännvidd mellan länder och inom länder, och det medför begräsningar – om vi inte kan beskriva problemet så kan det vara svårt att förstå problemet och det blir ännu svårare att lösa det. Inom det militära finns det i högre utsträckning ett gemensamt språk där de nordiska länderna bygger terminologi, begrepp, procedurer och praxis på Natos ramverk. Två exempel att inspireras av:

- *Forsvarets Etterretningsdoktrine 2021* (Norge) är ett bra exempel på hur man inom ett land tagit fram ett gemensamt språk.
- *Terminology Working Group* vid StratCom COE vars arbete syftar till att utveckla en gemensam terminologi inom området strategisk kommunikation. Ett mer exakt, men också enklare språk som överbryggar terminologin mellan beslutsfattare, militär, teknikföretag, akademiker och programmerare.

7. Strategisk kommunikation

Strategisk kommunikation är en betydelsefull förmåga för att bygga motståndskraft liksom i genomförandet av motåtgärder. **Ett utökat nordiskt samarbete i syfte att koordinera och förstärka strategiska insatser kan ha stor effekt.** Dels för att attribuera illegitim påverkan och avskräcka främmande makt, dels för att säkra intern och extern sammanhållning. Exempel på gemensamma insatser kan vara:

- Förstärk gemensamma kommunikationen inför, under och efter gemensamma militära och civila övningar och insatser.
- Skapa ett protokoll för snabba stöduttalande vid olika hybridangrepp där främmande makt pekas ut.
- Utvisning av diplomater bör ske koordinerat och i solidaritet som svar på angrepp mot nordiska demokratiska institutioner och nationella säkerhetsstrukturer.[51]
- Etablering och vidmakthållande av strategiska narrativ. Vi skriver själva berättelsen om hur vi ska försvara våra land. De nordiska länderna behöver enskilt och tillsammans möta destruktiva narrativ från främmande makt och andra antagonister genom att proaktivt etablera och vidmakthålla egna narrativ.

De nordiska länderna kommer utifrån sina medlemskap i EU och Nato delvis att ha olika säkerhetspolitiska överväganden och prioriteringar, men **det finns fortfarande mer som förenar oss än som skiljer oss**.

8. Riskkommunikation och transparens

De nordiska ländernas hantering av pandemin påvisar behovet av att utveckla förmågan till riskkommunikation. **Proaktiv kommunikation innan och under en kris som bygger på välgrundade målsättningar, målgruppsanalyser och angreppssätt, samt att kontinuerligt utvärdera egen kommunikation och varna för pågående desinformation.** På alla nivåer behövs arbete för att proaktivt möta potentiella brister och informationsvacuum som kan uppstå. Två aktuella exempel på det är:

- Den pågående pandemin har visats sig vara en grogrund för konspirationsteorier och extremism. Illasinnade aktörer utnyttjar på olika sätt människors oro, rädsla och besvikelse för att växa sig starkare – för att öka föraktet mot politiker och offentliga institutioner.[52]
- Enligt Gränshinderrådet så har pandemin påvisat att de som bor och arbetar i gränsregionerna drabbats oskäligt hårt av ländernas olika restriktioner och gränsstängningar. Därav har rådet lyft att de nordiska länderna behöver ta fram en plan för hur de negativa effekterna för gränsboende kan minskas vid likande kriser i framtiden.[53]

Nationella riskbedömningar som *Risiko 2021* och nationella säkerhets- och underrättelsemyndigheters öppna årsredovisningar är goda exempel när det gäller riskkommunikation och transparens. Men de är punktinsatser och **det behövs ökad kontinuitet och intensitet**:

- Risker och hotbilder som lyfts fram i dessa rapporter behöver kommuniceras i större omfattning och över tid.
- Genom att utveckla, samordna och förstärka nationell och nordisk riskkommunikation kan befolkningen förberedas för framtida kriser och potentiella informationsvacuum begränsas.

9. Utbildning

Ökad medvetenhet bidrar till motståndskraft och utbildning är ett viktigt verktyg för detta. Etablera **samverkan och samarbete för merutbyte av olika utbildningar och genomförandet av gemensamma utbildningar inom olika områden och på olika nivåer**. Från basal nivå för ett brett spektrum av målgrupper, till specialistutbildningar för de som arbetar operativt med att identifiera och möta påverkansoperationer och desinformation:

- Media- och informationskunnighet (inklusive digital källkritik, sökkritik och källtilit).
- Grundläggande medvetenhet kring risker, sårbarheter och hotbild kopplat till påverkansoperationer och desinformation.
- Identifiera och möta desinformation utifrån verktyg som *RESIST* och *The ABCDE Framework*.
- OSINT (informationsinhämtning genom öppna källor) och digital forensik (analys av elektroniska spår).

Det finns många digitala plattformar och nätverk för utbildning och kunskapsspridning, några exempel att inspireras av är:

- Det europeiska samarbetet EDMO – United against disinformation.
- Global Engagement Center (GEC) som är en del av US State Department. Deras arbete är till stor del nätverksbaserat och de står som värd för en mängd bra initiativ som exempelvis *Disinfo Cloud*.
- First Draft Training.
- *Internetkunskap.se* av Internetstiftelsen.

10. Övning

Öva mera och utveckla samverkan på området. Det för att lära av varandra och för merutbyte av upplägg och övningsmaterial. Om vi inte övar så är det svårt att lyckas hantera de potentiella hot som kan uppstå – hur ska olika aktörer och sektorer vara förberedda och ha förmåga att möta exempelvis en kognitiv överbelastningsattack[54, 55] om de aldrig övat på det?

- Öka inslagen av påverkansoperationer och desinformation i mindre såväl som större övningar när det kommer till krishantering och beredskap.
- Involvera fler civila aktörer i militära övningar och fler militära i civila övningar. Öka fokus på militär-civil samverkan, på nationell nivå och över landsgränserna.
- Utveckla scenarier. Scenarier som kan möjliggöra både en tydligare kravställning gentemot enskilda myndigheter och bidra till en sammanhängande gemensam problemformulering och planering. Utifrån framtagna scenarier så går det att genomföra tvärsektoriella övningar nationellt liksom i olika nordiska forum.
- Etablera en gemensam digital plattform för övning och träning. Det finns pågående projekt hos bland annat Forsvarets forskningsinstitutt (utveckling av simuleringsplattformar med öppen källkod med "kloner" av sociala medier) som kan användas i ett nordiskt sammanhang.

Slutnoter

1. Iam, M. S., Sarkar, T., Khan, S. H., Mostofa Kamal, A., Hasan, S. M. M., Kabir, A., Yeasmin, D., Islam, M. A., Amin Chowdhury, K. I., Anwar, K. S., Chughtai, A. A., & Seale, H. (2020): *COVID-19–Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis* – The American Journal of Tropical Medicine and Hygiene, Volume 103 Issue 4 (ajtmh.org).
2. Jesper Lehto (2021): *Vaccinkampen: Så sprids desinformationen om coronavaccinet* – Frivärld (frivarld.se).
3. Rory Smith, Seb Cubbon, Claire Wardle (2020): *Under the surface: Covid-19 vaccine narratives, misinformation and data deficits on social media* – First Draft (firstdraftnews.org).
4. James Pamment, Howard Nothhaft, Henrik Agardh-Twetman, Alicia Fjällhed (2018): *Countering Information Influence Activities The State of the Art* – MSB (msb.se).
5. Samantha Bradshaw, Hannah Bailey, Philip N. Howard (2021): *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* – DemTech (ox.ac.uk).
6. Fojo Medieinstitutet (2020): *Det nya normala – ett hot mot demokratin* – Medieinstitutet Fojo (fojo.se).
7. Patrik Oksanen (2020): *Kinas attacker för att tysta kritiker* – Frivärld (frivarld.se).
8. Stratcom COE (2021): *Abuse of power: coordinated online harassment of Finnish government ministers* – StratCom (stratcomcoe.org).
9. Sebastian Bay (2020): *9 Psykologiskt försvar – förebyggande i fokus*, Rapportsammanfattning – Totalförsvarets forskningsinstitut (foi.se).
10. StratCom COE (2020): *Social Media Manipulation Report 2020* – StratCom (stratcomcoe.org).
11. Forbrukerrådet (2020): *Out of Control* – Forbrukerrådet (forbrukerradet.no).
12. StratCom COE (2020): *Data Brokers and Security* – StratCom (stratcomcoe.org).
13. Global Disinformation Index (2020): *Ad Tech and Disinformation in the EU* – GDI (disinformationindex.org).
14. Rory Smith, Liliana Bounegru, Jonathan Gray (2021): *How anti-vaccination websites build audiences and monetize misinformation* – First Draft (firstdraftnews.org).
15. James Vincent (2020): *This is what a deepfake voice clone used in a failed fraud attempt sounds like* – The Verge (theverge.com).
16. Dagens Nyheter (2021): *Falska svenska marina fartyg på nätet* – Dagens Nyheter (dn.se).
17. Anders Danielsson, Maguns Hjort, Stina Wessiling (2020): *En ny myndighet för att stärka det psykologiska försvaret* – SOU 2020:29 (regeringen.se).
18. Patrik Oksanen (2021): *Pandemin är en perfekt kris att exploatera* – Kvartal (kvartal.se).
19. Torbjørn Kveberg, Vårin Alme, Sverre Diesen (2019): *Defence against foreign influence – a value-based approach to define and assess harm, and to direct defence measures* – Forsvarets forskningsinstitutt (ffi.no).
20. Säkerhetskommittén, Finland (2017): *Säkerhetsstrategin för samhället, Statsrådets principbeslut* – Säkerhetskommittén (turvallisuuskomitea.fi).
21. Stratcom COE (2019): *Hybrid Threats: A Strategic Communications Perspective* – StratCom (stratcomcoe.org).
22. Anders Danielsson, Maguns Hjort, Stina Wessiling (2020): *En ny myndighet för att stärka det psykologiska försvaret* – SOU 2020:29 (regeringen.se).
23. Regjeringen, Danmark (2018): *Udenrigs- og Sikkerhedspolitisk Strategi 2019-2020* – Udenrigsministeriet (um.dk).
24. Anders Danielsson, Maguns Hjort, Stina Wessiling (2020): *En ny myndighet för att stärka det psykologiska försvaret* – SOU 2020:29 (regeringen.se).
25. Regjeringen, Norge (2019): *Ti tiltak for hindre uønsket påvirkning i valggjennomføringen* – Kommunal- og moderniseringsdepartementet, Justis- og beredskapsdepartementet (regjeringen.no).
26. Regjeringen, Norge (2020): *Samfunnssikkerhet i en usikker verden* – Meld. St. 5 (2020–2021) (regjeringen.no).
27. Europeiska kommissionen (2016): *Gemensamt meddelande till Europaparlamentet och Rådet: Gemensam ram för att motverka hybridhot* – Europeiska kommissionen (eur-lex.europa.eu).
28. Europeiska Rådet (2019): *Complementary efforts to enhance resilience and counter hybrid threats* – Europeiska Rådet (data.consilium.europa.eu).

29. Europeiska Rådet (2019): *Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats* – Europeiska Rådet (data.consilium.europa.eu).
30. Europeiska Rådet (2019): *En ny strategisk agenda 2019-2024* – Europeiska Rådet (consilium.europa.eu).
31. Europeiska kommissionen (2021): *European Democracy Action Plan* – Europeiska kommissionen (ec.europa.eu).
32. Europeiska kommissionen (2021): *The Digital Services Act: ensuring a safe and accountable online environment* – Europeiska kommissionen (ec.europa.eu).
33. Regjeringen, Norge (2020): *Norway has responded to the European Commission concerning the regulation of digital platforms* – Ministry of Local Government and Modernisation (regjeringen.no).
34. EEAS (2021): *Countering disinformation* – EEAS (eeas.europa.eu).
35. Government, UK (2021): *MCDC Countering hybrid warfare project: understanding hybrid warfare* – Ministry of Defence (gov.uk).
36. Nordiska rådet (2018): *Så bekämpar Norden fake news* – Nordiskt samarbete (norden.org).
37. Nordocom (2018): *Fighting Fakes – The Nordic Way* – Nordicom (nordicom.gu.se).
38. Myndigheten för samhällsskydd och beredskap (2018): *Så bygger vi säkerhet i Norden: Ett svenskt myndighetsperspektiv* – MSB (msb.se).
39. Nordiska rådet (2020): *Fake news och demokrati tema på Nordiska rådets temasession* – Nordiskt samarbete (norden.org).
40. Statsrådet, Finland (2019): *Beredskap för och mötande av informationspåverkan som tema för Finlands och Sveriges gemensamma övning* – Statsrådets kommunikationsavdelning (valtioneuvosto.fi).
41. Myndigheten för samhällsskydd och beredskap (2018): *Att möta informationspåverkan – Handbok för kommunikatörer* – MSB (msb.se).
42. Nordiska rådet (2020): *Nordicom samordnar nytt forum för MIK-forskning* – Nordicom (nordicom.gu.se).
43. NordMedia Network (2021): *NordMedia Conference 2021* – NordMedia Network (nordmedianetwork.org).
44. NORDIS network on online disinformation (2021): *Online Disinformation: an Integrated View* – NORDIS (nordis.research.it.uu.se).
45. Sebastian Bay (2020): *9 Psykologiskt försvar – förebyggande i fokus*, Rapportsammanfattning – Totalförsvarets forskningsinstitut (foi.se).
46. Nordiska rådet (2021): *Nordiska rådet vill se mer utrikes- och säkerhetspolitiskt samarbete* – Nordiskt samarbete (norden.org).
47. Nordiska rådet (2021): *Kan krissamarbetet i Norden bli bättre?* – Nordiskt samarbete (norden.org).
48. Nordiska rådet (2019): *Nordisk råds strategi for samfunnssikkerhet* – Nordisk råd (norden.diva-portal.org).
49. Björn Bjarnarson (2020): *Nordic Foreign and Security Policy 2020*, Proposals July 2020 – Utenriksdepartementet (regjeringen.no).
50. King's College London (2021): *Security Studies academics contribute to UK government's foreign policy and defence review* – King's College London (kcl.ac.uk).
51. Patrik Oksanen (2021): *Extra: Stortinget utsatt för ny attack* – Frivärld (frivarld.se).
52. Svenska Dagbladet (2021): *Expert: De känner sig bedragna av en "elit"* – SvD (svd.se).
53. Nordiska rådet (2021): *Gränsregioner drabbas – nio av tio upplever ökad oro av coronarestriktioner* – Nordiskt samarbete (norden.org).
54. Waniek, Marcin, Raman, Guru Raghav, Alshebli, Bedoor, Peng, Jimmy, Rahwan, Talal (2020): *Traffic networks are vulnerable to disinformation attacks* – ResearchGate (researchgate.net).
55. Raman, Guru Raghav, AlShebli, Bedoor, Waniek, Marcin, Rahwan, Talal, Peng, Jimmy Chih-Hsien (2020): *How weaponizing disinformation can bring down a city's power grid* – Plos One (journals.plos.org).

Om författaren

ANTON LIF

Anton Lif är specialist på informationspåverkan och kommunikation, och fagprofil i UTSYN. Idag arbetar han som Crisis Management-konsult på Combitech, ett oberoende bolag inom försvars- och säkerhetskoncernen Saab. Under många år arbetade Anton vid Försvarsmaktens förband för psykologiska operationer (psyops), där han varit med och utvecklat förmågan i Sverige.

UTSYN – FORUM FOR UTENRIKS OG SIKKERHET

Stortorvet 3
0155 Oslo

www.prosjektutsyn.no

post@prosjektutsyn.no

Fagnotatet er tilrettelagt og publisert med støtte fra Utenriksdepartementet og Fritt Ord.