Begreppet hybrida hot

av Sophie Mandahl

Résumé

The development of the security environment during the last decade has been complex and includes kinetic and non-kinetic threats. This has led to the emergence of several concepts, such as "hybrid threats", "grey zone" or "hybrid warfare". The activities often include political influence, disinformation, cyberattacks, sabotage, economic pressure, and support to extremist groups. This raises the question of which concept is best suited for describing the current situation. Is there a risk that certain concepts create more anxiety and uncertainty than calm and comprehensibility? There may be situations where a trade-off must be made. What takes precedence: The need for conceptualization or the risk of confusion and indirect support of the enemy's agenda? It seems like the concept "hybrid threat" is the most suitable to describe the current situation. However, it should not be used casually to label every single incident, as that can exaggerate the enemy's capacity and spread fear. Instead, the term is most valuable at a strategic level, to describe patterns and cumulative effects, support legal and policy development, and help the public understand what is happening without amplifying the adversary's narrative.

DET SENASTE DECENNIETS, och inte minst de senaste fyra årens säkerhetspolitiska utveckling, har varit obehaglig och svår att greppa för många. Informationslandskapet präglas av ett högt tempo, öppna och dolda påverkansaktiviteter, samt ett överflöd av tillgängliga kanaler, vilka kan vara allt ifrån myndigheters kommunikation, till traditionella nyhetsmedier, till sociala medieplattformar.

Den säkerhetspolitiska utvecklingen har gett upphov till användningen av flertalet begrepp för att beskriva den verklighet vi befinner oss i. Några exempel är hybrida hot, gråzonsproblematik och hybridkrigföring. Inget av de nu nämnda begreppen har någon enhetlig allmänt vedertagen definition. Exempel på sådant som vanligtvis innefattas i begreppen är politisk påverkan, desinformation, cyberangrepp, fysiskt sabotage, informationspåverkan, ryktesspridning, manipulering av marknader, strategiska uppköp, maktdemonstrationer av militärt eller annat slag, stöd till ytterlighetsrörelser i landet, illegal underrättelseinhämtning, samt hot och påtryckningar mot beslutsfattare. Ofta är det en kombination av olika aktiviteter och det kan vara oklart vem eller vad som ligger bakom dem.

Det finns ett behov hos individer och hos samhället i stort att definiera och kategorisera företeelser för att skapa förståelse och förklara händelser. Det har gjorts försök att åstadkomma begrepp som ska uppnå just det, med mer eller mindre lyckad framgång. Olika begrepp har tillkommit medan andra har försvunnit vilket visar på behovet av att ha ett samlingsbegrepp för potentiellt kumulerande och sammanhängande händelser. Det framstår som att det finns en begränsad livslängd för nya begrepp. Det mest sannolika är att begrepp byts ut, frågan är bara när och mot vad. Vidare är det svårt och tids-

krävande att definiera dessa begrepp, och det saknas kanske skäl att göra det utanför den akademiska sfären. Samtidigt kan ett visst begrepp vara användbart och fylla ett syfte för tillfället varför det kan vara nyttigt att använda det.

Det finns anledning att sätta ord på vad vi blir utsatta för, dels för att förstå och sätta det i ett sammanhang, dels för att kunna agera mot det. Utifrån ett juridiskt perspektiv är uppdelningen mellan krig och fred väsentlig eftersom olika verktyg blir tillämpliga för det som kategoriseras in under hybrida hot. Gemensamt för de flesta misstänkta påverkansoperationer eller händelser som kategoriseras in under ett begrepp är att de hamnar under nivån för det folkrättsliga begreppet väpnad konflikt. Det gäller även när de har bekräftats och attribuerats, d v s att det är fastställt vem som ligger bakom.

Frågan är vilket eller vilka begrepp som bäst lämpar sig för ändamålet. Finns det en risk att vissa begrepp skapar mer oro och ovisshet än lugn och greppbarhet? Det kan finnas situationer där en avvägning måste göras. Vad får företräde: behovet av konceptualisering eller risken för förvirring och att gå motståndarens ärenden?

Motståndaren

I Europa eftersträvar vi en regelbaserad världsordning vilket kan göra oss sårbara eftersom våra motståndare har ett annat synsätt, en annan agenda och ett annat tillvägagångssätt. I första hand är det Rysslands agerande som brukar innefattas i begreppet hybrida hot, men även Kina och Iran är aktörer som använder sig av liknande metoder.

Med andra medel än kinetiska söker fienden successivt vänja oss vid dess närvaro och att vi bara ska rycka på axlarna för sådant som tidigare hade rört upp starkare reaktioner. Det handlar om att påverka och förändra samhället så att kontroll uppnås. Små steg i en särskild riktning blir till slut en typ av dominans. Slutmålet är att genom tillåtna eller icke förbjudna medel uppnå inflytande i skydd av vår rättsstat och våra demokratiska värderingar. Genom att infiltrera och utnyttja de strukturer som finns i Sverige kommer främmande makt åt kontroll på ett lagligt sätt.

En stor skillnad sedan den fullskaliga invasionen av Ukraina 2022 är att det sker fler riktade aktiviteter och att de sker med mindre försiktighet. Organisationer såsom GRU (Rysslands militära underrättelsetjänst) brukar mer våld, exempelvis genom riktade mord, och utför sabotage i större utsträckning och mer oförsiktigt. Ett exempel är det planerade mordet av Armin Papperger, vd för den tyska försvarskoncernen Rheinmetall, som dock kunde avvärjas.[1]

> *Det handlar om att påverka och förändra samhället så att kontroll uppnås.*

Ryssland, Kina och Iran vill utmana och sänka förtroendet för Nato och EU och gör detta genom hybrida hot eller alternativa påverkansvägar i syfte att skapa ovisshet, tvivel och rädsla. En strävan är att påverka befolkningen så att tilliten till den egna staten minskar. Med sina hybrida metoder försöker motståndaren sudda ut linjen mellan krig och fred. En uppfattning som funnits och kanske fortfarande finns i Sverige är att fred är ett tillstånd mellan stater som helt saknar någon typ av fientlig aktivitet. Samtidigt uppfattas motsatsen krig som en företeelse som bedrivs i full skala och helt öppet. Det är viktigt att inte fastna i den föreställningen utan att i stället vara medveten om att agerande som kategoriseras under

beteckningen hybrida hot med stor sannolikhet alltid kommer att fortgå.

Vad är det som försiggår?

Ett medel som används är olika former av cyberattacker. Dessa utförs inte sällan av statsaktörer och deras ombud, eller proxy som det heter på engelska. Ombuden kan vara kriminella nätverk som agerar på uppdrag av främmande makts underrättelsetjänst. Incidenter med skadade eller förstörda undervattenskablar är ett annat exempel.

Påverkanskampanjer utgör ytterligare en grupp av handlingar. Dessa kan vara kampanjer som riktas direkt mot grupper i landet, till exempel LVU[2]-kampanjen som syftade till att undergräva invandrargruppers förtroende för den svenska staten genom att sprida falska rykten om att socialtjänsten på felaktiga grunder tvångsomhändertog muslimska barn. Där blev det tydligt att traditionella nyhetskanaler inte alltid är den viktigaste informationskällan för alla samhällsgrupper. Mycket av informationen spreds via sociala medier.[3]

Ett annat exempel är otillbörlig informationspåverkan som i olika mer eller mindre försåtliga former placeras hos journalister eller i alternativa kanaler, såsom sociala medier, där de kan spridas vidare. Då handlar det om att så tvivel om information från svenska staten eller andra överstatliga aktörer. Syftet är att skapa en ovisshet och att vilseleda beslutfattare och befolkningen i landet. Ytterst handlar det om att påverka vår kognitiva förmåga för att få oss att tappa förmågan att fatta beslut, alternativt att få oss att vara den som tar till militära medel först.

Aktiviteter eller handlingar som främmande makt utför har stora likheter med hur olika underrättelsetjänster agerade under kalla kriget, exempelvis den politiska krigföring som den då sovjetiska kommittén för statens säkerhet (KGB) genomförde. Det som kännetecknar dessa attacker och handlingar är att ingen tar på sig ansvaret som angripare. Det gör att det blir svårare att bemöta och agera mot sådana handlingar. Metoden är betydligt mer kostnadseffektiv, både ekonomiskt och politiskt, än konventionellt militärt våld och har potential att få mycket stora effekter.

Doppelgänger, en fälla i dubbel bemärkelse

En brist i begreppsfloran är risken med att ge företeelser häftiga namn såsom ”Doppelgänger”, som betyder dubbelgångare på tyska. Uttrycket syftar på en gigantisk Kreml-ledd påverkansoperation som ska bidra till att Ryssland når sina säkerhetspolitiska målsättningar i Ukraina och runtom i världen. Begreppet beskriver en operation som blev ökänd för att skapa kloner av legitima webbplatser i syfte att sprida desinformation. Den inkluderar nyhetssajter, statliga webbplatser och en mängd andra pro-ryska och anti-ukrainska plattformar. Innehållet stärks ofta med falska individer på sociala medier såväl som med betalda annonser.[4]

> *Att bli omtalad är framgång.*

Det beskrivs som att påverkansoperationer som Doppelgänger upptäcks som intressanta enskilda öar av information, och att det vid upptäckandet sällan finns bevis på strategisk nivå. Ur ett strategiskt perspektiv är dock Doppelgänger ingen viktig taktik. Det är dessutom ingen operation. Det är en metod som Russian Social Design Agency (SDA) använder sig av för att få ut information och den upptäcktes nästan lika snabbt som den startades. Frågan om SDA:s egentliga syfte

dyker upp direkt. Den verkliga framgången för Kreml är de 350 nyhetsartiklarna som florerat internationellt om Doppelgänger. Dessa ger en enorm effekt och avkastning på den investering som SDA gjort och genererar troligtvis fler resurser från Kreml i syfte att genomföra andra liknande kampanjer. Ur ett ryskt perspektiv är det en mycket lyckad påverkanskampanj till stor del på grund av uppståndelsen kring densamma. Att bli omtalad är framgång. Att upptäckas är framgång. Att bli faktakollad, avfärdad eller fördömd är framgång. Att upprepas av politiker, kändisar och trovärdiga nyhetskällor är framgång. Framgång eftersom det skapar ovisshet och rädsla, för något som inte är lika storartat som det framstår.[5]

Skrota gråzonsbegreppet

Begreppet ”gråzon” används för att beteckna handlingar som försiggår i gränssnittet mellan krig och fred. Vanligtvis brukar handlingarna beskrivs som icke-kinetiska, alltså utan direkt fysisk kraft. Det är främmande makt som nyttjar fientliga maktmedel såsom desinformation, cyberattacker eller sabotage för att påverka ett lands beslut utan att utlösa ett fullskaligt krig.

Begreppet gråzon är missvisande. Användningen av begreppet gråzon för att särskilja ett tillstånd från fred kan göra att vi blir blinda för att relationen med Ryssland de senaste decennierna har utgjorts av en hård och aggressiv form av fred. Det finns en tendens att intala sig att fred är ett vänligt tillstånd vilket riskerar att förleda oss i att det som nu sker i det som kallas gråzon är nytt och således inte har förekommit tidigare. För ett ryskt säkerhetsetablissemang är fred med fientliga inslag inte något exceptionellt. Det anses vara normala mellanstatliga relationer.

För det första är fred sällan helt i avsaknad av fientliga handlingar varför det i så fall skulle vara gråzon den största delen av tiden. Alltså skulle tillståndet fred i princip bara finnas i teorin om vi väljer att använda begreppet gråzon.

För det andra kan användningen av begreppet gråzon, särskilt i kombination med begreppet skymningsläge, göra att tillståndet ses som en tidslinje. Skymningsläge symboliserar att mörkret är på väg, vilket ökar risken för att stirra sig blind på att nästa steg kommer att ligga närmare krig än det som sker i dagsläget. Det kan förleda oss att inte se alternativa scenarion.

För det tredje gynnar gråzonsbegreppet fiendens narrativ. Det skapar oro och ovisshet att klumpa samman allt till begreppet gråzon, som en oförståelig grå klump av incidenter som verkar obehagliga, vilket är exakt vad främmande makt vill uppnå.

Hybrida hot och hybridkrigföring

Begreppen hybrida hot och hybridkrigföring har fått ett stort genomslag i den säkerhetspolitiska debatten under det senaste decenniet. Begreppet hybridkrigföring myntades ursprungligen av forskaren Frank Hoffman som en beskrivning av Hizbollahs uppträdande under kriget mot Israel 2006. Det utmärkte sig som en blandning av okonventionell gerillataktik och konventionell krigföring vilket ansågs avvika från gängse uppfattning om hur icke-statliga aktörer opererar.

Efter Rysslands annektering av Krim och efterföljande dolda invasion av östra Ukraina 2014 har begreppet hybrida hot uteslutande kommit att användas som en samlingsbenämning för hur statliga aktörer, framför allt Ryssland, men även Kina och Iran, nyttjar och kombinerar olika maktmedel mot sina motståndare på den internationella arenan. Syftet är, som nämnts tidigare, att påverka politiskt beslutsfattande och förmågor, att

förstärka samhälleliga sårbarheter, samt bidra till destabilisering, polarisering, osäkerhet och minskad tillit till det egna politiska systemet och samhället i stort.

Enligt Europeiska kompetenscentret för motverkande av hybrida hot (Hybrid CoE) kännetecknas hybrida hot av att de utgör ”1) Koordinerade och synkroniserade handlingar som avsiktligen inriktas mot sårbarheter i demokratiska staters och institutioners system genom en stor bredd av medel. 2) Aktiviteter som exploaterar dels trösklar för upptäckt och attribuering, dels gränssnitten mellan krig och fred, inrikes och utrikes säkerhet, lokal och nationell nivå, samt den nationella och internationella politiska nivån. 3) Aktiviteter som syftar till att påverka olika former av beslutsfattande lokalt, regionalt och statligt, samt inom internationella organisationer, och är utformade för att uppnå aktörens strategiska målsättningar samt att underminera eller skada den som utsätts.” [Egen översättning][6]

> *De flesta krig och allvarliga konflikter i världshistorien har utkämpats med någon form av kombination av konventionella och okonventionella maktmedel och kan därför sägas vara hybrida.*

Hybrida hot kan handla om asymmetriska strategier eller konflikter för att åstadkomma nationella mål från länder såsom Ryssland, Kina, Iran och Nordkorea. Det finns även icke-statliga aktörer som kan sägas använda sig av metoderna, exempelvis ISIS och Hizbollah. Exempel på antagonistiska ageranden som ofta diskuteras i termer av hybrida hot, alternativt i singularformen hybridhot, är sabotage, påverkansoperationer, cyberattacker, tvingande eller villkorsbetingad diplomati, samt utnyttjande av ekonomisk beroendeställning. Hybrida hot kan vara tvärsektoriella och kombinera handlingar inom en rad olika områden såsom de tretton som Hybrid CoE beskriver [egen översättning]: infrastruktur, cyber, rymden, ekonomi, militär och försvar, kultur, socioekonomi och samhälle, offentlig förvaltning, juridik, underrättelse, diplomati, politik, information.[7]

Bara faktumet att det finns ett europeiskt kompetenscenter för motverkande av hybrida hot talar för att begreppet är här för att stanna. Dock finns det vissa brister med begreppen hybrida hot och hybridkrigföring.

Kritik

Användningen av begreppet krigföring för att beskriva något som kan ske längs hela hotskalan, framförallt för sådant som sker i fredstid, är problematisk. Ytterligare ett problem med användningen av hybrida hot är att det är ett brett och allomfattande begrepp vilket riskerar att förvirra och göra händelserna svårförståeliga snarare än konkreta och greppbara. Det är också vanligt att begreppet hybrida hot i huvudsak används för att beskriva Rysslands agerande gentemot demokratiska stater. Det gör att begreppet förlorar i kraft när det gäller att beskriva olika länders verksamhet och blir således svårare att använda för att på ett universellt plan förklara de händelser som vi blir utsatta för.

Ett ytterligare argument är att de flesta krig och allvarliga konflikter i världshistorien har utkämpats med någon form av kombination av konventionella och okonventionella maktmedel och kan därför sägas vara hybrida. Begreppet omfattar alltså ingenting nytt, utan betecknar sådant som pågått i alla tider i mellanstatliga relationer. Diskussionen om hybrida hot reflekterar kan-

ske främst ett uppvaknande inom västvärlden om att mellanstatliga relationer kan präglas av motsättningar snarare än samarbete, exempelvis mellan EU och Ryssland. Till följd av att Ryssland utnyttjat vår naivitet, i kombination med den snabba tekniska utvecklingen, har vi utvecklat reella sårbarheter.[8]

Som ett uttryck för uppvaknandet har en rad liknande begrepp uppkommit vid sidan om hybridkrigföring för att beskriva säkerhetshoten. Begreppen står inför likartad problematik: det är en utmaning att utveckla en gemensam och okontroversiell definition som fångar den komplexitet som präglar de hot och sårbarheter vi möter. Exempel på snarlika begrepp som förekommit i litteraturen är *Sixth Generation Warfare*, *Contactless warfare*, *New warfare*, *Next-generation warfare*, *Ambiguous warfare*, *Asymmetrical warfare*, *Non-linear warfare*, samt *Full Spectrum Conflict*.[9]

Juridiken är tydlig: dikotomin krig och fred

I svensk rätt är det antingen krig eller fred. Hybrida hot hittar man både under fredstid och i krig. Uppdelningen mellan krig och fred är väsentlig eftersom olika verktyg blir tillämpliga för det som kategoriseras in under hybrida hot. I krig är juridiken förhållandevis tillåtande, och syftar till att avgöra om en incident innefattas i krigföringen och om militära styrkor är tillåtna att agera mot den. Det grundar sig i folkrättsliga regler som kallas krigets lagar. I fred är det ordinarie regler som gäller. De incidenter som sker hanteras och utreds utifrån de gärningar som är belagda med straff i lag. Dessutom är det i fredstid relevant för regeringen att göra en sammantagen bedömning av flera på varandra ackumulerande händelser för att kunna ta beslut om politisk inriktning och om landet ska övergå till gällande regler för krig eller krigsfara.

Omslagspunkten för regler om bland annat krig och krigsfara är när regeringen beslutar om höjd beredskap, alternativt förklarar att riket är i krig. Fram till dess ska alla incidenter som vi blir utsatta för hanteras i enlighet med de ordinarie regler som finns i fredstid. Det innebär att Polisen förebygger, förhindrar och utreder brott som sedan avgörs i domstol. Vidare är det upp till lagstiftaren att avgöra om det ska finnas ett juridiskt stadium mellan fred och krig. Därför finns det i fredstid en anledning att skapa en samlad bild av hur främmande makt försöker eller lyckas påverka Sverige och svenska intressen. Lagstiftaren bör ta den säkerhetspolitiska utvecklingen i beaktande för att kunna stävja hotande verksamhet genom lag om förbud eller straff för vissa gärningar. Svensk rätt är på ett sätt en spegling av samhällets bild av moral och vad som är rätt och fel. Återspeglingen är inte alltid korrekt beroende på vem man frågar. Dessutom är kanske speglingen inte dagsaktuell med tanke på att lagstiftningsprocessen inte sker över en natt. Och det ska den så klart inte heller göra, eftersom lagstiftning bör vara långsiktig och inte impulsiv. Det kan vara svårt att uppnå en aktuell spegling i en värld som förändras på veckor, om inte dagar eller till och med timmar. Därför kan det vara relevant att kategorisera in händelser under begreppet hybrida hot för att förstå vad det är som hotar och på vilket sätt. Lagstiftaren kan då använda begreppet hybrida hot för att konceptuellt förstå och hänga med i utvecklingen för att sedan stifta lagar därefter. Ett exempel på ny lagstiftning som tillkommit delvis för att hindra främmande makt från att utnyttja hål i svensk lagstiftning är lagen (2023:560) om granskning av utländska direktinvesteringar som kom den 21 september 2023. Den

innebär en möjlighet att hindra utländska direktinvesteringar i svensk skyddsvärd verksamhet. Värt att notera är att den inte kan tillämpas retroaktivt på grund av grundläggande rättsliga principer.[10]

Det finns idag inget brott eller något juridiskt begrepp som benämns hybrida hot. Den lagstiftning som kan användas för att hantera det som benämns för hybrida hot är exempelvis brotten sabotage, spionerі, och skadegörelse enligt brottsbalken (1962:700), eller brott mot vapenlagen (1996:67). Vidare kan det även röra sig om terroristbrott enligt lagen (2003:148) om straff för terroristbrott. Alltså kan det ur ett brottsperspektiv vara överflödigt och till och med förvirrande att prata om hybrida hot eftersom det inte är ett brott. Möjligen skulle man kunna se en framtida lagstiftning mot hybrida brott som idag finns gällande terroristbrott. Alltså att lagstiftaren väljer att kriminalisera det hybrida elementet i brottet så som terrorism anses förstärka en redan brottslig gärning.

I takt med att hoten mot Sverige byter skepnad och blir alltmer överlappande, kan det utöver ny lagstiftning krävas andra metoder för brottsbekämpning. Att hoten byter skepnad kan innebära att gränserna mellan gängkriminalitet, terror och främmande makts påverkan suddas ut. Exempelvis kan främmande makt påverka och agera genom ombud som kan utgöra kriminella gäng som enbart motiveras av att tjäna pengar. Med tanke på detta är det i många fall svårt att avgöra vem som ligger bakom en viss händelse, om det ens finns någon som ligger bakom. Ur en motståndares perspektiv kan det finnas anledning att göra det svårt för oss att klargöra vem som ligger bakom, eller rentav få det att framstå som att det var slumpen. Ibland kanske motståndaren till och med tar på sig en incident för att gynnas av händelser som egentligen var slumpmässiga. Vidare kan det vara svårt att utröna motivet till incidenten. En person som fått ett uppdrag mot betalning kanske inte vet själv vad det egentliga syftet med agerandet är. I sådana fall kan det vara nästintill omöjligt att attribuera och hitta det egentliga motivet. På grund av dessa svårigheter är det synnerligen besvärligt och mångfacetterat för den som ska bekämpa alla hot.

För att få en gärning hanterad av polis och bedömd av domstol krävs att incidenten uppmärksammas eller rapporteras. Vem som bär ansvaret att göra det är inte helt klart. Det skulle kunna vara den som upptäcker det eller den som äger eller kontrollerar en viss verksamhet. Ett sådant ansvar kräver att individer, företag och myndigheter är väl insatta och uppdaterade på vilka typer av hybrida hot som kan förekomma. Dessutom är det inte helt klart vad ansvaret att agera ska innebära. Räcker det att anmäla till en ansvarig myndighet? Eller krävs det att ett företag vidtar förebyggande åtgärder såsom att närmare undersöka och sedan avböja en hyresförfrågan på grund av märkliga kopplingar till Ryssland? Och i så fall, hur långt ska en sådan efterforskning sträcka sig? Det går att argumentera för att en individ bör anmäla misstanke till lämplig myndighet och att ett företag bör avböja en misstänkt förfrågan. Däremot är det troligtvis svårt att upprätta juridiska krav på ett så långtgående ansvar. Ett exempel på lagstiftning där företag måste ta ställning är utländska investeringar. Lagen (2023:560) om granskning av utländska direktinvesteringar som nämndes tidigare är ett tydligt exempel på att en lucka i lagen har hanterats med ny lagstiftning. Ett annat exempel på lagstiftning som skapar ytterligare skydd från främmande makts hot är lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS). Den här typen av regler är en signal från lagstiftaren att det finns anledning att vara på sin vakt, samtidigt som

lagstiftningen inte på något sätt är ett heltäckande skydd. I brist på juridiska regler om ansvar finns det anledning att uppmärksamma potentiella hot. Därför kan det vara användbart med begreppet hybrida hot för att sprida medvetenhet och skapa förståelse för exempelvis företag och individer om vad de bör vara vaksamma mot.

Lära av Finland?

I svensk rätt är krisberedskap och totalförsvar två uppdelade system där omslagspunkten är kopplad till höjd beredskap. Krisberedskap består av ordinarie regler för att hantera incidenter, medan totalförsvar omfattar flera olika lagar som skapar verktyg som tillkommer när beredskapen höjs. I den finska ordningen är det som utgångspunkt tänkt att ordinarie lagar och regler ska användas för att hantera kriser. Avsteg från det ordinarie förfarandet kan göras i vissa undantagsfall som återfinns i den finska beredskapslagen. Sedan våren 2022 kan hybrida hot anses innefattas i vad som utgör anledning att hantera en allvarlig kris enligt den finska beredskapslagen. Förändringen gjordes på grund av Rysslands fullskaliga invasion i Ukraina och innebär att hybrida hot är ytterligare en typ av undantagstillstånd som kräver särskilda regler.[11]

Vidare är Finland en förebild när det kommer till samhällets motståndskraft. Landet har sedan 2017 hamnat på första plats i European Media Literacy Index som mäter hur sårbara länder är mot desinformation. Enligt Open Society Institute, som är utgivare av indexet, visar en hög ranking på att samhället har bättre resiliens mot inverkningar av desinformation och liknande fenomen. Sverige hamnar på femte plats efter Danmark, Norge och Estland.[12] Några anledningar till att Finland har ett bra motstånd mot desinformation beskrivs med att stora delar av befolkningen är högutbildade samt att utbildningen håller en hög nivå. Dessutom är kritiskt tänkande en del av undervisningen i grundskolan.[13]

Det finns exempel på myndigheter, organisationer och företag i Finland som arbetar mot desinformation. Ett exempel är ett center för förebyggande av informationspåverkan inom den finska Försvarsmakten. Centret ordnar utbildning för Försvarsmaktens personal och reservister för att de ska lära sig att identifiera och förebygga all form av informationspåverkan.[14]

Vidare är finska myndigheter snabba med att korrigera propaganda som sprids via sociala plattformar. Ett exempel på detta är att rysk propaganda försökte få det att verka som att ryska trupper transporterades vid finska gränsen, varför en finsk myndighet avvisade detta och påpekade att bilderna var tagna i en annan kontext vid en annan tidpunkt. Informationen spreds direkt via Finlands public service-mediebolag Yle:s förstasida.[15]

> *Finland verkar vara bäst i klassen på att hantera hybrida hot såsom desinformation.*

Det finns också exempel på hur Finland hanterar sådana händelser som skulle kunna sorteras in under hybrida hot. En rysk affärsman köpte flertalet öar i Åbos skärgård där motivet gick att ifrågasätta. Finsk domstol dömde gärningsmannen för grovt skattebedrägeri och grovt bokföringsbrott. Det hela benämns som Airiston Helmi-härvan och är ett exempel på hur finska staten lyckas lagföra verksamhet som skulle kunna betraktas som hybrida hot. Genom att döma personen för andra brott hindras den potentiellt otillåtna verksamheten.[16]

Finland verkar vara bäst i klassen på att hantera hybrida hot såsom desinformation. Även om Sverige också anses vara i toppskiktet, kan det finnas lärdomar och mönster att ta efter.

Kommunikation och användning

Nyhetskonsumtionen har förändrats drastiskt bara de senaste 5–10 åren. Idag finns det en generation som i stor utsträckning erhåller nyheter via sociala medier. Många av dessa nyhetskonsumenter är sådana som tidigare inte läste tidningar eller lyssnade på nyhetssändningar. Den som öppnar Tiktok eller Instagram exponeras för ett flöde fyllt med allt ifrån gulliga kattungar till videoklipp från kriget i Ukraina. Det är en blandning mellan sant och falskt, men också en blandning mellan nyheter och underhållning. Detta beror på att applikationens flöde skapas av algoritmer som syftar till att få användaren att stanna kvar och scrolla vidare. Effekten blir att användaren blir en mer passiv mottagare av information.[17]

En effekt av den förändrade nyhetskonsumtionen kan vara att individer vill ha svar på frågor som uppkommit efter att ha sett något under sitt scrollande. Därför är det av största vikt att myndigheter och traditionella nyhetsmedier finns tillgängliga som ett ärligt och riktigt alternativ till sociala medier. Ett bra exempel som nämndes ovan är när Yle gick ut och dementerade förekomsten av trupptransporter vid finska gränsen.

Kommunikation kring händelser som kategoriseras in under hybrida hot handlar om att göra en avvägning mellan att rapportera och sprida information samtidigt som man vill minimera risken för att sprida information som missgynnar Sverige och vår säkerhet. Risken innebär att användningen av begreppet hybrida hot kan tillskriva motståndaren en strategi som inte finns, alternativt oavsiktligt sprida någon annans narrativ. Ett exempel på ett riskabelt tillvägagångssätt är sensationsjournalistik, som kan beskrivas med att fokus ligger på att få flest klick eller att vara snabbast med att rapportera om något. Ivrigheten riskerar att förblinda oss från det sakliga rapporterandet och att det kan finnas en dold agenda med händelsen som rapporteras. Det kan också vara så att det inte finns någon dold agenda. Användningen av hybrida hot i ett tidigt skede utan bekräftade uppgifter utgör ett exempel på sensationsjournalistik som riskerar att sprida motståndarens narrativ eller tillskriva en strategi som inte finns.

Det kan också krävas en noggrann kontroll av källans trovärdighet och motiv. Ett exempel på att potentiellt driva fel narrativ är rapporteringen om de skadade kablarna i Östersjön. Innan det finns faktiska bevis på att det är främmande makt som ligger bakom så finns det anledning att avvakta och inte lägga hela pusslet direkt. Att påstå att detta utgör misstänkt sabotage eller att kalla det för ett hybridhot kan vara att gå angriparens ärenden. Om det var angriparens gärning har denne lyckats med att sprida informationen och fortsatt inte vara avslöjad. Om det inte var angriparen har vi lyckats skapa en rädsla och oro för att angriparen skulle kunna ta till sådana medel trots att denne inte gjort någonting. Oavsett vad har vi gått i fällan. Det förekommer ofta uttalanden som just beskriver händelser som hybrida hot eller misstänkt sabotage. Det är kanske inte fel men det kan innebära att vi går motståndarens ärenden.[18]

I kris och krig behöver befolkningen information som går att lita på. Det kräver att myndigheter är trovärdiga och tillförlitliga i sin kommunikation. Det är viktigt att samla och presentera information för att öka medvetenheten hos befolkningen. Därför kan det

vara relevant att framhålla faktorer som att främmande makt försöker påverka oss och våra val. Det är svårt att fastställa exakt var gränsen går för att informera utan att sprida en överdriven bild av vad som sker. Att kommunikationen bör innehålla bekräftade fakta och väl granskade källor är inte omvälvande. Ju mer konkreta fakta och bevis som finns, desto mindre risk att gå angriparens ärenden. Tydlighet skapar visshet och greppbarhet medan ovisshet skapar oro.

För operativa myndigheter kan avvägningen handla om att få ut rätt information i rätt tid utan att förstöra en eventuell utredning eller operativ verksamhet. Det går att diskutera huruvida vi vill agera eller reagera. Bör vi försöka förekomma eventuella incidenter eller reagera på sådant som skett. Självklart är det eftersträvansvärt att förekomma incidenter och stoppa dem redan innan de sker. Det kan dock vara svårt och ibland omöjligt. Ett problem när vi inte vet vem som ligger bakom en händelse är att det tillkommer risker om vi går ut med våra spekulationer. Om det visar sig att det inte stämmer riskerar man att underminera sin egen trovärdighet.

Enskilda händelser bör tydligt beskrivas för vad de är tills något annat är fastställt. Begreppet hybrida hot är gynnsamt som ett samlingsbegrepp eller vid kategorisering av flera händelser, men inte som en beskrivning av en specifik händelse. Hybrida hot kan användas ur ett bredare perspektiv, till exempel i en årsöversikt eller i en strategisk analys.[19]

Vidare kan information om att det skulle kunna finnas inblandning från främmande makt tas emot olika beroende på vem som läser. En individ som arbetar med frågorna har kanske i större utsträckning en försiktig inställning till information som sprids och vem som ligger bakom. Kanske är experter mer misstänksamma på grund av att de potentiellt har mer bakgrundsinformation och kännedom om främmande makt och dess tillvägagångssätt. Däremot är det inte säkert att gemene man inte har samma förmåga. Hur välutbildad och inläst individen är påverkar den källkritiska förmågan. Det verkar finnas en stark tillit till traditionella nyhetsmedier när det gäller att hålla sig uppdaterad vid allvarliga kriser i Sverige. En undersökning visar att 60 % av svenskarna först vänder sig till en nyhetssajt eller nyhetsapplikation via mobil eller dator för att sedan komplettera inhämtningen av flera andra källor.[20]

Det bästa sättet att motverka desinformation eller påverkanskampanjer är att ha en välinformerad befolkning som tar eget ansvar avseende att vara källkritisk. Därför är det positivt att källkritik är en del av utbildningen i grundskolan. Därtill är det viktigt med trovärdiga medier och trovärdig information från myndigheter. Kommunikation bör präglas av bekräftade fakta och tydlighet kring vad som är bevisat och vad som är spekulation. Huruvida begreppet hybrida hot används eller ej är inte avgörande men det kan finnas bättre och sämre situationer för att nyttja begreppet. På ett konceptuellt plan är det gynnsamt att använda begreppet hybrida hot, medan det i enskilda fall finns anledning att fokusera rapporteringen på sådant som är bekräftat. Då stärker vi demokratin och befolkningens möjlighet att själv ta ansvar för sin uppfattning om läget.

Diskussion om hybrida hot, idag och i morgon

Idag är hybrida hot det vanligaste samlingsbegreppet inom EU och Nato för hot som inte innebär ett direkt militärt angrepp. Inom EU:s handlingsplan för säkerhets- och försvarspolitik, den strategiska kompassen från 2022, fastslogs att EU ska ta fram en verktygslåda för hybrida hot.[21] Det kan vara

problematiskt om definitionen av dessa inte är enhetlig. Nato omnämnde redan 2016 hybrida hot som en potentiell utlösande faktor för artikel 5. Samtidigt förklarar Nato:s strategiska koncept från 2022 att hybrida hot har en framträdande roll i Rysslands politik mot alliansen och omnämner arbetet för att stärka motståndskraften mot dessa som en prioritet.

Mot bakgrund av Rysslands fullskaliga invasion av Ukraina 2022 är en annan vanlig invändning att det fokus som diskussionen om hybrida hot har fått i den säkerhetspolitiska debatten har bidragit till en falsk trygghet. Man menar att den genererat en dominerande föreställning om att konflikten mellan Ryssland och västvärlden främst skulle utspelas i gråzonen mellan krig och fred och att risken för ett konventionellt krig även fortsatt skulle vara obefintlig. Det ska i sin tur ha bromsat nödvändiga satsningar på militärt försvar och försvarsindustri. Även om det sannolikt ligger en del i detta resonemang, får den bristande beredskapen inför utvecklingen i Ukraina främst ses som ett utslag av en begränsad imaginär och politisk förmåga snarare än en stundtals förvirrad begreppsdiskussion.

Det finns inte heller något i konceptet hybrida hot som utesluter användningen av konventionella militära maktmedel för att uppnå politiska syften, d v s krig, även om det stundtals framförts argument om att risker och kostnader med denna typ av maktutövning gör den mindre trolig. Istället söker begreppet hybrida hot synliggöra en bred palett av maktmedel tillgängliga för en antagonistisk aktör antingen som betydligt mer kostnadseffektiva alternativ, eller som förstärkande komplement, till konventionella militära förmågor. Hybrida medel kan, men måste inte, användas för att bana vägen för ett framgångsrikt militärt angrepp.

Det är värt att notera att Rysslands angrepp på Ukraina omfattat, och fortsätter att omfatta, en lång rad icke-kinetiska komponenter integrerat med den militära, inklusive politisk subversion, påverkansoperationer, ekonomiska maktmedel och cyberangrepp, där olika metoder varit olika framträdande över tid. Dessutom nyttjas dessa inte bara mot Ukraina utan även mot länder som stödjer Ukrainas försvarskamp. Att motsvarande palett av metoder är aktuella i Rysslands mellanhavanden med Nato är inte särskilt överraskande, dels eftersom Ryssland anser att kriget i Ukraina är en konflikt med Nato, dels eftersom Ryssland inte gör någon tydlig gränsdragning mellan konventionella och icke-konventionella metoder.

> *Det är just i den strategiska analysen av en motståndares kombinerade förmågor och hur dessa kan inriktas mot egna sårbarheter som begreppet hybrida hot är som mest användbart.*

Således betecknar hybrida hot ett brett och svårhanterligt spektrum av säkerhetspolitiska problem som likväl kan påverka alla nivåer av ett samhälle och därmed kräver kunskap och åtgärder. Det är också i detta avseende som konceptet i sig och debatten kring detsamma varit mest verkningsfulla. Insikten att antagonistiska aktörer kan kombinera en rad olika maktmedel för att underminera västerländska stater var långt ifrån självklar före 2014. Detta har i sin tur bidragit till en bredare analys av samhälleliga sårbarheter och ökad förmåga att förstå dessa i ett sammanhang.

Det är just i den strategiska analysen av en motståndares kombinerade förmågor och hur dessa kan inriktas mot egna sårbarhe-

ter som begreppet hybrida hot är som mest användbart. I dagens offentliga samtal benämns ofta allt från misstänkta sabotage mot undervattensinfrastruktur till främjande av migrationsströmmar, till kampanjer för informationspåverkan som hybridattacker, vilket inte alltid är särskilt klargörande. Istället erbjuder begrepp som hybrida hot konceptuella ramar för att analysera hur dessa, kanske synbarligen isolerade, händelser hänger samman i ett större perspektiv som innefattar en motståndares strategi och hur denna kan motverkas och förebyggas.

Det är av vikt att hitta en balans i användandet av begreppet hybrida hot. Å ena sidan att inte använda det i fall där begreppet riskerar att tillskriva mer strategi än vad som faktiskt föreligger. Å andra sidan att sätta flera händelser i ett sammanhang för att bättre förstå helheten.

När hybridhot används för att beskriva en enskild händelse finns det en risk att vi uppmuntras att se mönster där det inte finns något sådant, eller att motståndaren har förmågor som den inte besitter. En risk är att motståndaren framstår som smartare och mer kapabel än vad den är. Det kanske egentligen bara är tillfälliga sammanträffanden. Ett sätt att se på detta är att fienden tar tillvara varje tillfälle att påverka, varför det framstår som att det finns en genomtänkt röd tråd. Och det kanske är just det narrativ som främmande makt vill sprida. Oavsett om främmande makt ligger bakom eller ej drar den nytta av det. Samtidigt kan vi inte undvika att belysa och försöka identifiera företeelser. Dock är det ju först när attribuering och motiv är fastställt som vi kan avgöra om det är främmande makt som legat bakom.

Det är också av vikt att fundera på vad främmande makt har för syfte. Det kan finnas ett annat mål än krig med tillvägagångssättet. Målet är kanske inte att bedriva ett fullskaligt krig, eller ens en operation med militärt våld. Målet och syftet är kanske istället att uppnå makt eller erövring genom politiskt, ekonomiskt eller juridiskt inflytande, så kallad *soft power*. Det kan vara en typ av psykologisk krigföring som syftar till att ändra åsikter och uppfattning till att gynna avsändarlandet. Kina använder sig av mjuk makt, eller diskursmakt som kineserna själva kallar det, d v s säga makt över ordens innebörd. Det syftar till att ändra uppfattningen om begrepp som exempelvis fred eller demokrati, till att få en innebörd som rimmar bättre med Kinas framgång och världsbild. Kina nyttjar det som en byteshandel där bistånd eller lån ersätts med exempelvis politiska beslut eller tillgång till information eller infrastruktur. Det kan även beskrivas som att Kina använder retoriken som vapen för att uppnå en multilateral värld där Kina är en avgörande stormakt. Dessutom agerar Kina fysiskt i Sydkinesiska havet och utgör ett hot mot Taiwan.[22]

I sammanhanget är det även relevant att ställa sig frågan: Vad framkallar mest rädsla och oro: Närvaro av styrkor eller frånvaro av svagheter? Främmande makt, i synnerhet Ryssland, arbetar uppenbarligen för att uppnå det förstnämnda, med alla typer av medel, såväl konventionella som okonventionella.

Slutsats

Mot bakgrund av att främmande makt använder andra maktmedel än militärt våld så har det uppkommit ett behov av att definiera och kategorisera händelser som sker gentemot Sverige. Olika begrepp har kommit och gått, somliga med större användningsområde än andra. Några begrepp som används idag är gråzon, hybrida hot och hybridkrigföring. Frågan är vilket eller vilka begrepp som bäst lämpar sig för ändamålet. Finns det en risk

att vissa begrepp skapar mer oro och ovisshet än lugn och greppbarhet?

Det finns anledning att minimera användning av begreppen gråzon och hybridkrigföring. Gråzon är ett missvisande begrepp, exempelvis eftersom det inte finns något mellanting mellan fred och krig. Det är mer relevant att diskutera fred som ett tillstånd med företeelser som inte är av vänlig karaktär. Vidare indikerar krig inom ramen för hybridkrigföring att det rör sig om något som är likt eller har att göra med krig, vilket inte alltid är fallet. Därför kan det vara missvisande att använda sig av dessa begrepp. Hybrida hot däremot kan förekomma i både krig och fred varför det skulle kunna vara ett lämpligare begrepp.

Det finns dock brister även med hybrida hot. Begreppet omfattar egentligen ingenting nytt utan sätter ord på händelser som förekommer i mellanstatliga relationer. Hybrida hot är brett och allomfattande vilket kan leda tankarna till att omfatta mer än vad begreppet faktiskt innebär. Dessutom är det riskabelt att slentrianmässigt kategorisera in varje enskild händelse under ett och samma begreppsparaply eftersom det kan tillföra händelsen ytterligare innebörd som kanske inte finns. Vidare är juridiken tydlig: det finns krig och det finns fred, inget däremellan. Det som benämns som hybrida hot försiggår både i krig och i fred. Hybrida hot är inget juridiskt begrepp men kan användas av lagstiftaren vid bedömning av vilka nya lagar som bör stiftas, samt av brottsbekämpande myndigheter för att få en helhetsbild av läget.

Begreppet hybrida hot har bidragit till insikten om att antagonistiska aktörer kan kombinera en rad olika maktmedel för att underminera västerländska stater, vilket inte var självklart före 2014. Nu verkar budskapet ha nått fram till den breda majoriteten, varför det finns anledning att nyttja begreppet hybrida hot mer restriktivt och mer strategiskt.

Vid beskrivning av en enskild händelse är begreppet hybrida hot inte lämpligt eftersom det styr in vårt tänkande på strategi och sammanhang som inte ryms inom en enskild händelse. Däremot lämpar sig begreppet hybrida hot för att beskriva läget på ett strategiskt plan. Hybrida hot skapar förståelse och greppbarhet när det används som ett koncept eller som en beskrivning av flera på varandra kumulerande händelser. Det gäller troligtvis även ifall motiv eller avsändare inte har fastslagits.

För att illustrera effekten av ett bra begrepp kan man tänka sig den obehagliga oroskänslan i en skräckfilm innan man fått se monstret eller skurken. Känslan försvinner så fort vampyren visar sig eftersom man då tänker att ”Jaha, det var bara en vampyr! Den vet vi hur vi ska bekämpa”. Den effekten kan begreppet hybrida hot ha vid förklaring av vad som sker och vad vi blir utsatta för, särskilt på ett strategiskt plan. Begreppet hybrida hot är den bästa lösningen på begreppsproblematiken, fram till dess att det ersätts med ett nytt begrepp.

Författaren är analytiker och verksam vid Försvarshögskolans Centrum för totalförsvar och samhällets säkerhet.

Noter

1. Lillis, Katie Bo, Bertrand, Natasha och Pleitgen, Frederik: "Exclusive: US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine", CNN, 2024-07-11, *https://edition.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot*, (2025-12-09).
2. Lagen (1990:52) med särskilda bestämmelser om vård av unga.
3. Ranstorp, Magnus och Ahlerup, Linda: "LVU-kampanjen: desinformation, konspirationsteorier, och kopplingarna mellan det inhemska och det internationella i relation till informationspåverkan från icke-statliga aktörer", Försvarshögskolan, Centrum för totalförsvar och samhällets säkerhet, 2023.
4. Pamment, James och Tsurtsumia, Darejan: *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency*. Myndigheten för psykologiskt försvar och Institutet för psykologiskt försvar vid Lunds universitet, 2025, *https://mpf.se/publikationer/publikationer/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency*, s 14.
5. Ibid, s 15 f.
6. Hybrid threats as a concept, Hybrid CoE, *https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/* (2025-12-08).
7. Giannopoulos, G. Smith, H. & Theocharidou, M: *The Landscape of Hybrid Threats: A Conceptual Model*, European Union and Hybrid CoE, Luxembourg 2021.
8. Nilsson, Niklas: *Sårbarheter i moderna samhällen blottläggs av hybrida hot*, Officerstidningen, 2024-06-24, *https://officerstidningen.se/sarbarheter-i-moderna-samhallen-blottlaggs-av-hybrida-hot/*, (2025-05-14).
9. Ibid.
10. Prop. 2022/23:116, s 19.
11. SOU 2023:75, s 309 ff.
12. Lessenski, Marin: "Finland Tops the New Media Literacy Index 2023, Countries Close to the War in Ukraine Remain Among the Most Vulnerable to Disinformation", 2023-06-24, *https://osis.bg/?p=4450&lang=en*, (2025-05-14).
13. Finnilä, Heidi: *Inte nog med att vi är lyckligast, finländare är också världsbäst i mediekunskap – För att upprätthålla kunskapen krävs medvetna satsningar och ständig uppdatering,* Yle, 2022-10-18, *https://yle.fi/a/7-10021855*, (2025-05-14); Saari, Dominic, Moilanen, Panu, och Hautala, Miriam: *The disinformation landscape in Finland,* University of Jyväskylä, 2023-05-08, *https://www.disinfo.eu/publications/disinformation-landscape-in-finland/*, (2025-05-19).
14. Fredriksson, Ann-Lis: *Försvarsmakten har fått ett center för förebyggande av informationspåverkan*, Yle, 2023-01-22, *https://yle.fi/a/7-10026996*, (2025-05-14).
15. Benke, Erika och Spring, Marianna: *US midterm elections: Does Finland have the answer to fake news?*, BBC news, 2022-10-10, *https://www.bbc.com/news/world-europe-63222819* (2025-05-14).
16. Fagerudd, David: *Riksdagsledamot Sandra Bergqvist om ryska markköp: "Vi kan inte vara lika blåögda längre"*, Yle, 2022-03-11, *https://yle.fi/a/7-10014034*, (2025-05-27), Lehtola, Johanna: *Airiston Helmi-rättegången: Mer tid för båda parterna att överklaga domen,* Yle, 2025-04-04, *https://yle.fi/a/7-10075660*, (2025-05-14).
17. Dalgard, Henrik: "Vi borde logga ut från Tiktok", Svenska Dagbladet, 2025-08-18, *https://www.svd.se/a/eMjwoO/vi-borde-logga-ut-fran-tiktok* (2025-08-18).
18. Granlund, John och Jönsson, Oskar: "60 hybridattacker mot Europa – spåren pekar mot Ryssland", SVT, 2025-03-12, *https://www.svt.se/nyheter/inrikes/60-hybridattacker-mot-europa-sparen-pekar-mot-ryssland*, (2025-06-26).
19. Ibid.
20. Ylä-Anttila, Merja och Stjärne, Hanna: "Yle och SVT: Public service stärker samhällets beredskap i allvarliga tider", Yle, 2023-07-03, *https://svenska.yle.fi/a/7-10037380*, (2025-05-15).
21. Den gemensamma säkerhets- och försvarspolitiken, GSFP, beskrivs närmare i bilagor till Lissabonfördraget, främst protokoll nr 1 (om de nationella parlamentens roll i Europeiska unionen), nr 10 (om det permanenta strukturerade samarbete som inrättas genom artikel 42 i EU-fördraget) och nr 11 (om artikel 42 i EU-fördraget) samt i förklaringarna nr 13 och 14 (förklaringar om den gemensamma utrikes- och säkerhetspolitiken).
22. Oud, Malin och Drinhausen, Katja (red.): *Decoding China Dictionary*, second edition, 2023.