FOI
Totalförsvarets forskningsinstitut

Hybrida hot

En introduktion för svenska aktörer

Hybrida hot

är subversiv verksamhet från främmande makt under tröskeln för krig med syfte att främja strategiska mål.

Sverige ställs idag inför ett nytt säkerhetspolitiskt hot. Det är svårt att upptäcka, eftersom vi har svårt att sätta ord på vad det handlar om. Denna broschyr syftar till att ge en sådan beskrivning av det som kallas **hybrida hot**.

Hybrida hot uppstår i tider av fred som präglas av aktörer i vår närmiljö som vill Sverige illa. Samtidigt som vi fortsätter bygga starka relationer med allierade stater, finns det också de som medvetet genomför insatser som på olika sätt försvagar Sverige som land.

I denna broschyr går vi närmare in på en beskrivning av hur hotet riktas mot Sverige som måltavla, hur hotet kan definieras, vad det är för typer av hot vi kan leta efter och hur vi kan tänka i de åtgärder som ska syfta till att värja oss från hybrida hots negativa konsekvenser.

Broschyren kan användas tillsammans med spelkortleken ”Att möta hybridhot” som tagits fram av RISE och Försvarshögskolan.

Demokrati
Fria val och politisk styrning med grund i svenska intressen.

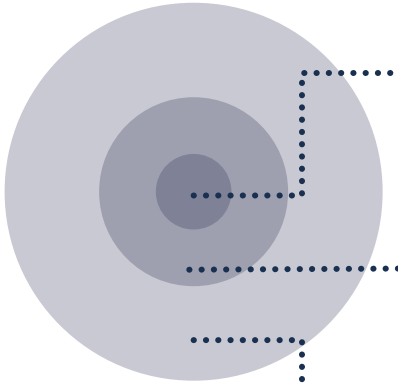
Kritisk infrastruktur
Som transportvägar och centrala trafikplatser, system för el- och vattenförsörjning.

Fri åsiktsbildning
Med tillgång till information och gemensamma samtal om samhällsviktiga frågor.

Gränser
Till land och havs, i luften och rymden.

Välfärd
Som skola, vård och omsorg, tillgång till bibliotek och kultur.

Tillit och förtroende
Till varandra, till myndigheter, rättsväsendet och det demokratiska systemet.



Du
Som en del av totalförsvaret kan du bli en måltavla för hybrida hot. Antingen genom riktade cyberangrepp för att få tillgång till lösenord och information, genom hatkampanjer för att tysta dig, eller på annat sätt påverka ditt beteende.

Din organisation
Den myndighet, kommun eller företag du jobbar på men även det trossamfund eller den lokala idrottsföreningen du är engagerad i kan bli en måltavla.

Ert verksamhetsområde
Du och de organisationer du är engagerad i är en del i ett större samtal kopplat till samhällsviktiga områden. På så sätt kan du eller din organisation bli föremål för attacker som har ett bredare syfte att skada Sverige.

Hybrida hot riktas mot hela svenska samhället

Hybrida hot riktar sig mot hela samhället, oavsett sektor. Speciellt utsatta är samhällsviktig verksamhet och aktörer eller system som har möjlighet att påverka beslutsfattande i Sverige.

Attackerna riktas mot såväl individer som organisationer och verksamhetsområden. Det innebär att alla har ett ansvar att arbeta för att upptäcka, larma och hantera hybrida hot.

Skydd för hela samhället

Totalförsvaret

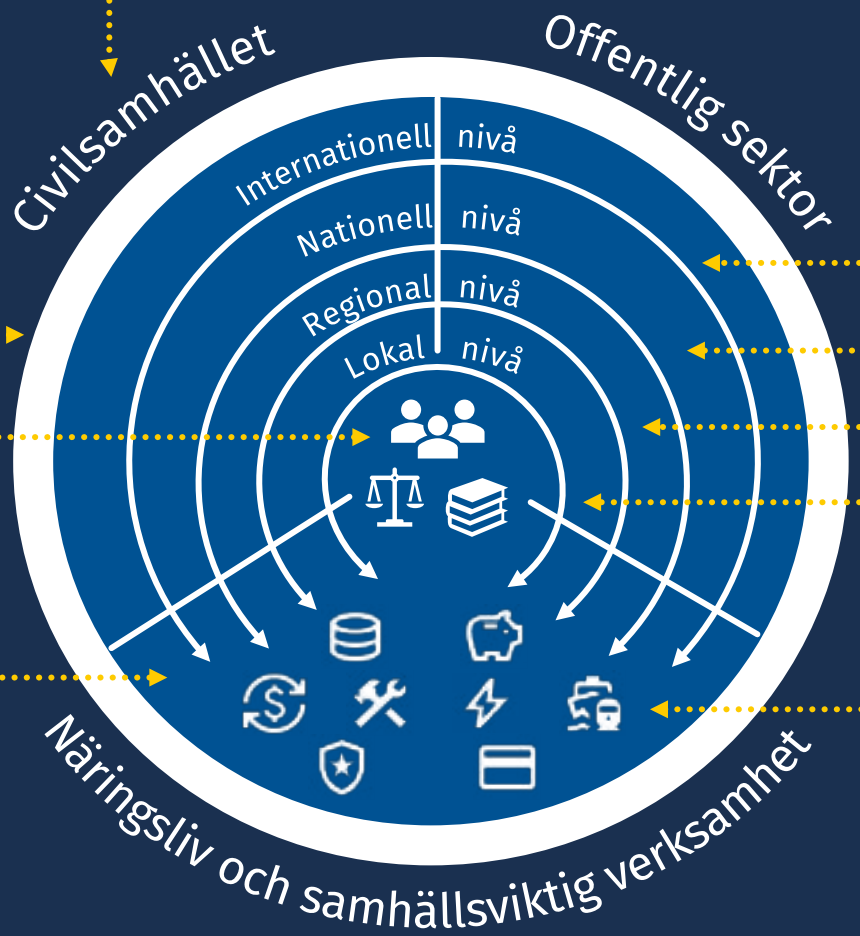
Skapar motståndskraft under fredstid, men aktiveras först under höjd beredskap.

Värden

Demokrati, rättsstaten, sammanhållning, tillit, språk och kultur.

Samhällsviktig verksamhet

Det finns vissa funktioner i samhället som håller upp våra gemensamma strukturer. Här samarbetar såväl offentlig sektor som civilsamhället och näringslivet. Det civila försvaret omfattas idag av 12 beredskaps-sektorer.



Civilsamhället

Religiösa samfund, frivillig-organisationer, fackförbund, idrotts- och kulturföreningar på såväl lokal som regional, nationell och internationell nivå.

Offentlig sektor

Internationellt EU, Nato och Sveriges bilaterala relationer.

Nationellt Myndigheter och departement.

Regionalt Regioner, länsstyrelser civilområden, polis- och militärregioner.

Lokalt 290 kommuner, Räddningstjänsten och andra lokala aktörer.

Näringsliv

Svenska företag som exempelvis driver samhällsviktig verksamhet såsom apotek och skolor, men även aktörer inom tillverkningsindustrin, banker, transportföretag och andra företag som är viktiga för Sverige i och utanför landets gränser.

Fyra kännetecken

Hybrida hot kännetecknas av fyra centrala dimensioner som tillsammans bygger vår förståelse om hotet mot Sverige.

Subversiv verksamhet
Hybrida hot är till sin natur destabiliserande och samhällsomstörtande genom att underminera samhälleliga institutioner och försvaga landets försvar.

Främmande makt
Hybrida hot drivs av andra stater, antingen genom den egna organisationen eller ombud. Angreppen är på så sätt styrda av främmande makt, men kan utföras av andra aktörer.

Under tröskeln för krig
Hybrida hot är inte krigshandlingar i folkrättslig mening, utan är strategiskt utformade för att undvika krig. Samma attacker kan ske i läge av krig, men då talar vi om hybridkrigföring.

Strategiska mål
Hybrida hot uppstår inte spontant. De bedrivs med syfte att nå mål som ligger i angriparens intressen. Det kan till exempel handla om att försvaga Sverige eller att minska vårt stöd till Ukraina.

Subversiv verksamhet

Hybrida hot är till sin natur destabiliserande och samhällsomstörtande genom att underminera samhälleliga institutioner och försvaga landets försvar.

Det definierande draget med hybrida hot är inte nödvändigtvis de specifika medel som används eller de mål som angrips, utan att avsikt och/eller effekt på ett eller annat sätt underminerar måltavlans kapacitet och/eller handlingsutrymme. Detta underminerande moment, som vi här kallar subversion, är centralt i värderingen av huruvida ett skeende är att bedöma som hybrid påverkan eller inte.

Oavsett om det rör sig om sabotage eller cyberattacker, kränkningar av luftrummet eller attacker mot kritisk infrastruktur i Sverige, präglas alltså hybrida hot av att de på ett eller annat sätt har en underminerande effekt eller att sammanhanget ger uttryck för att operationen har ett sådant syfte från hybridaktörens sida.

Ytterst kan denna subversiva verksamhet drivas till väpnade angrepp mot Sverige, där hybrida hot sänker tröskeln genom att försvaga landets försvar.

Främmande makt

Hybrida hot drivs av andra stater, antingen genom den egna organisationen eller ombud. Angreppen är på så sätt styrda av främmande makt, men kan utföras av andra aktörer.

Den mest centrala faktorn av betydelse för hanteringen av hybrida hot är kunskap den utförande aktören. Aktörsperspektivet är alltså centralt för förståelsen av hybrida hot.

Ageranden för att påverka andra länder kan ske på många olika sätt med både öppna och dolda metoder. Hybrida angrepp med öppna metoder kan omfatta allt från diplomatiska kampanjer, ekonomisk påtryckning, militära provokationer, offentligt stöd för antidemokratiska rörelser m.m. De är lättare att identifiera och därmed också lättare att förhålla sig till.

Dolda hybrida angrepp sker i de flesta fall med resurser och metoder som medför att angreppet blir svårt att både upptäcka och attribuera till anstiftaren bakom angreppet. Dolda metoder medför osäkerhet, både om vad som skett och vem som står bakom.

Under tröskeln för krig

Hybrida hot är utformade för att inte anses vara krigshandlingar i folkrättslig mening, utan för att falla under gränsen. Samma attacker kan ske i läge av krig, men då kallas detta för hybridkrigföring.

Stater använder sig regelmässigt av både öppna och dolda, lagliga och olagliga, konventionella och icke-konventionella, civila och militära metoder för att skaffa sig fördelar gentemot andra stater och uppnå sina mål. Krig uppstår när regeringen utlyser att man är i krig. Det innebär att tillståndet baseras på en bedömning av läget som råder, där hybrida hot strategisk håller sig under gränsen för vad som anses vara en krigshandling. Samtidigt utesluter inte Nato att hybrida hot kan utlösa artikel 5.

I samband med krig aktiveras en ny uppsättning lagar, som alltså inte gäller i normalläget och inte heller inom ramen för hybrida hot. Det innebär att Sveriges bemötande behöver hålla sig inom ramarna för vad vi har mandat att göra i fred, vilket gör det viktigt att utnyttja lagens offensiva och defensiva kraft.

Strategiska mål

Hybrida hot bedrivs med syfte att uppnå mål som ligger i angriparens intressen. Det kan handla om mål som att försvaga Sverige eller stärka det egna landets position.

Precis som konsekvenserna med hybrida hot är att Sverige försvagas som land präglas också hybrida hot av att intentionen är att uppnå ett för angriparen strategiskt intresse. Det kan röra sig om en bred uppsättning intressen, där intentionen kan vara att skada Sverige eller på andra sätt förstärka den egna positionen och uppnå nationella mål.

Säkerhets- och försvarspolitiska målsättningar är på sätt och vis det minst komplicerade kriteriet i definitionen av hybrida hot. Detta eftersom de regelbundet kommuniceras i strategidokument eller av politiska beslutsfattare.

Beroende på land har olika aktörer olika strategiska målsättningar. Det är därför viktigt att kontinuerligt bevaka och uppdatera hotbilden som riktas mot Sverige.

Koordinerade attacker

Hybrida hot är ofta utformade för att inte bli upptäckta. Därför är det inte bara viktigt att känna till vilka typer av angrepp det kan röra sig om, men också bygga strukturer för att kunna se mönster i helhetsbilden.

I vissa fall uppträder hybrida hot som uppenbara händelser, såsom dataintrång med utpressningsförsök eller diplomatiska påtryckningar och restriktioner. I andra fall rör det sig om kampanjer på sociala medier under falska identiteter, industrispionage genom systematiska stölder av affärshemligheter eller förgiftning av dricksvatten. För att upptäcka hybrida hot behöver vi därför ha förmåga att samla en gemensam lägesbild som avslöjar hur dessa händelser kan tänkas hänga ihop.

Exempel på hybrida hot

Information och kognition
- Desinformation och propaganda
- Mediepåverkan
- Falska identiteter och nätverk
- Läckor för påverkan
- Karaktärsmord

Cyber och rymd
- Överbelastningsattacker
- Utpressningsangrepp
- Datastöld och cyberspionage
- Störning av GPS och navigering
- Störning av satellitkommunikation

Ekonomi och finansiella beroenden
- Strategiska investeringar
- Handelspåtryckningar och restriktioner
- Industrispionage

Fysisk infrastruktur och logistik
- Sabotage mot kablar och rörledningar
- Störning av energiförsörjning
- Angrepp mot industriella system
- Manipulation av logistik och transporter
- Drönare över skyddade områden
- Biologiska angrepp

Rättsstat, politik och offentlig förvaltning
- Utnyttja rättsliga processer
- Exploatera administrativa svagheter
- Korruption
- Hot och påtryckningar mot beslutsfattare
- Dolt stöd till politiska aktörer
- Valpåverkan

Diplomati och internationell påverkan
- Påtryckningsdiplomati
- Rörelserestriktioner
- Underminera tillit till partners
- Påverkan i internationella forum

Underrättelseverksamhet
- Spionage och underrättelseinhämtning
- Rekrytering av agenter och informanter
- Infiltrering av organisationer
- Paramilitära och kriminella ombud
- Mord och mordförsök
- Provokation genom territoriella kränkningar
- Militär signalering och övningar

Sveriges målsättningar

Vårt samlade svar på hybrida hot grundas i den nationella säkerhets-strategin.

Sverige behöver öka förmågan att hantera hybrida hot. Den skapas dels genom strukturer för att identifiera och hantera hoten, men också genom att på förhand åtgärda sårbarheter och därigenom göra det svårt för motståndaren att angripa svenska mål. Sådana insatser kan i sin tur inte bara höja vår beredskap och förmåga att försvara oss, men också avskräcka angripare från att attackera Sverige.

Vårt samlade svar på hybrida hot grundas i den nationella säkerhetsstrategin. Sveriges nationella säkerhetsintressen ser du till höger. Du hittar den nationella säkerhets-strategin på regeringen.se.

1. Värna Sveriges säkerhet, demokratiska styrelseskick, frihet, självständighet, suveränitet och handlingsfrihet
2. Värna befolkningens liv och hälsa
3. Försvara Sverige och våra allierade mot väpnat angrepp och upprätthålla vår territoriella integritet
4. Upprätthålla försörjningsberedskap och samhällets funktionalitet
5. Upprätthålla våra grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter

Reaktivt eller proaktivt

Bemötandet av hybrida hot omfattar åtgärder när något har hänt eller med hänsyn till vad som skulle kunna hända.

Reaktiva åtgärder genomförs efter att en händelse inträffat. Då behöver beträffade aktörer agera snabbt och tillsammans för att skapa en lägesbild av vad som har inträffat och vad den underliggande strategin kan vara. Reaktiva åtgärder kan också bestraffa en motståndare i avskräckande syfte. Kom ihåg att en förväntad reaktion kan också spela in i aktörens strategiska intressen, och följas av nya attacker.

Proaktiva åtgärder sker innan en händelse upptäckts för att skapa större motståndskraft mo eventuella angrepp. Utgångpunkt kan vara risk- och sårbarhetsanalyser såväl som säkerhetstjänsternas beskrivning av främmande makts intressen. Proaktiv signalering av vidtagna åtgärder kan också användas för att avstyra en angripare från att attackera den egna verksamheten.

Offensivt eller defensivt

Offensiva åtgärder riktar sig mot den som bedriver hybrida hot, defensiva åtgärder stärker det egna systemet.

Offensiva åtgärder riktar sig mot de som agerar mot Sverige. Det kan antingen röra sig om åtgärder riktade direkt mot de som utför hybrida hot, eller mot de förutsättningar som möjliggör motståndarens agerande.

Defensiva åtgärder har fokus på det egna systemet. De kan handla om att skydda centrala resurser från skada eller att se till att kritisk infrastruktur inte slås ut.

Defensiva åtgärder utgör grunden i hanteringen av hybrida hot. Det är också viktigt att samverka med andra svenska och internationella aktörer för att dela lärdomar och erfarenheter som kan bygga en starkare helhet.

Fyra strategityper mot hybrida hot

Med utgångspunkt i de två dimensionerna kan vi dela in åtgärder i fyra strategier.

Beskyddande strategier har som mål att upprätthålla den egna förmågan och skydda samhällsviktig verksamhet när påfrestningar uppstår.

Konfrontativa strategier har som mål att avskräcka fienden genom att lägga stor vikt vid vedergällning efter att ett angrepp har konstaterats.

Bemötande strategier har som mål att agera självständigt i relation till hotbilden för att på så sätt undvika att påverkas av hybrida hot.

Störande strategier har som mål att påverka motståndaren innan hybrida hot blir ett faktum. Det kan exempelvis gälla att begränsa dennes förmåga eller att störa kommunikationsvägar.


Reaktiv
Proaktiv
Defensiv
Offensiv
Förstärkt lagstiftning mot hybrida hot
Lagföring av hotaktörer
Stärkt skalskydd
Informationsinsats från myndighet
Skydd vid övningar och transporter
Säkerhetsprövning och personskydd
Incidentberedskap vid kränkningar
Stärkt krisledningsförmåga
Valskydd och -säkerhet
Intern kontroll och antikorruption
Tvärsektoriell samverkan
Beslagta resurser
Samordnat internationellt narrativ
Kontraspionage
Eskalationsstyrning och signalering
Offensiv tillämpning av folkrätt
Gräns-, sjö- och luftövervakning
Show of force
Koalitionsbyggande och alliansolidaritet
Gemensam underrättelseverksamhet
Rättslig beredskap och kapacitet
Beredskapsplanering och övning

En liten parlör för hybrida hot

Hybrida hot eller **hybridhot** (plural) definieras som ”subversiv verksamhet från främmande makt under tröskeln för väpnat angrepp med syfte att främja dennes strategiska målsättningar”. Det är en samlingsbeteckning på de offensiva strategier, verktyg och åtgärder som kan användas för att underminera och/eller försvaga en motståndare.

Den eller de som effektuerar hybrida hot, såväl som dennes beställare eller överordnade, kan betecknas som en **hybrid aktör**. Exempelvis kan såväl staten Ryssland såväl som dess underrättelsetjänst KGB betraktas som hybridaktörer.

Hybrida aktörer kan utföra **hybridangrepp, -operationer** eller **-aktiviteter** mot ett mål eller målobjekt (dessa används oftast synonymt). Målet utsätts då för **hybrid påverkan**.

Motståndskraft är förmågan hos en aktör eller grupp av aktörer att reducera effekten av hybridangrepp, helt eller delvis.

Resiliens är förmågan hos en aktör eller grupp av aktörer som utsätts för hybrid påverkan att vara motståndskraftig(a) och dessutom snabbt kunna återgå till tillståndet som föregick hybridangreppet. Notera att ”resilience” i exempelvis Nato-sammanhang har en mer övergripande betydelse.

Hybridkrig eller **hybridkrigföring** är en eskalering från hybrida hot. Hybridkrigföring kan vara både en förberedelse för konventionella angrepp, eller utgöra en integrerad del av krigföringen i samband med en väpnad konflikt. Detta betecknar då användandet av icke-konventionella metoder, eller kombinationer med konventionella sådana, för att besegra fienden. Det är då i princip synonymt med begrepp som ”modern krigföring” eller ”nya generationens krigföring”.

En **strategi** för hantering av hybrida hot är en övergripande plan för hur en aktör, eller grupp av aktörer, ska förhindra eller motstå hybridangrepp. En strategi kan beskriva vägledande förhållningssätt, verktyg och åtgärder.

Denna broschyr ger en introduktion till hybrida hot och hur aktörer i Sverige kan förstå om och i sådana fall på vilket sätt de kan drabbas.

För mer information om vilka verktyg som kan användas i bemötandet av hybrida hot, se **foi.se**.

Totalförsvarets forskningsinstitut 2026