Moderaternas reformagenda mot hybridhot

Det väpnade angreppet är fortsatt utgångspunkten för att bygga svensk försvarsförmåga. De ryska kraven på att Sverige inte ska få göra sina egna säkerhetspolitiska vägval har dock satt fingret på att vi också behöver en rad nya verktyg för att möta bredden av andra hot såsom cyberattacker, sabotage, valpåverkan, desinformationskampanjer och fientliga uppköp – så kallade hybridhot.

Den gemensamma nämnaren för dessa hot är de ofta verkar i gråzonen mellan den totala freden och det totala kriget. Sveriges säkerhet måste därför byggas utifrån en målbild om ett motståndskraftigt samhälle där alla delar samverkar och där vi är bättre rustade för att möta såväl kris, krig och hybridattacker i gråzonen mellan fred och krig.

En moderatledd regering kommer att driva en reformagenda för att stärka Sveriges förmåga att möta den flerdimensionella hotbild som vårt land står inför idag. En sådan reformagenda kommer att utgöra en del av en ny nationell säkerhetsstrategi. Det handlar bland annat om följande förslag:

1. Ta fram en offensiv strategi i förhållande till de utländska underrättelseofficerare som agerar på svensk mark.

2. Tillsätt en utredning som har till uppgift att göra en total översyn av svensk strafflagstiftning i relation till hybridhoten. Utredningen bör bland annat lämna förslag på hur det straffbara området ska utökas för att fånga in alla relevanta hybridhot samt föreslå straffskärpningar.

3. Ge Försvarsmakten och Polisen i uppdrag att ta fram en samlad strategi för att möta hotet från drönare.

4. Ändra signalspaningslagen för att tillåta signalspaning även om både avsändare och mottagare befinner sig i Sverige.

5. Återupprätta den särskilda beredskapspolisen för att stärka Sveriges möjligheter att möta hybridhot även i fredstid.

6. Ändra lagstiftningen så att Försvarsmakten ges möjlighet att stödja Polisen vid extraordinära händelser och tillse att Försvarsmakten kompenseras resursmässigt för denna nya uppgift.

7. Få granskningssystemet för utländska direktinvesteringar på plats så snart som möjligt och se till att det finns en tillräcklig finansiering för att det ska fungera effektivt.

8. Säkerställ att Säpo har tillräckligt med resurser för att arbeta med att utbilda och stödja det svenska näringslivet i arbetet med säkerhetsskyddslagen.

9. Gör en översyn av hur samhällsviktiga företag kan få särskilt stöd av underrättelse- och säkerhetstjänsterna för att kunna upptäcka och motverka spionage och attacker mot sin verksamhet.

10. Kartlägg de policydokument som statliga bolag och institutioner använder sig av och som riskerar att få negativa effekter på svensk förmåga och säkerhet.

11. Begränsa det kommunala självstyret i frågor som berör nationell säkerhet genom att införa ett statligt kontrollsystem av t.ex. hamnar och flygplatser

12. Kartlägg det utländska ägandet av antagonistiska stater i den svenska industrin

13. Grunda ett nationellt cyberförsvarscampus, med egna utbildnings- och forskningsresurser och ett uppdrag att stödja såväl försvaret, civila myndigheter och näringslivet med kompetensförsörjning

14. Inrätta en cyberkoordinator på det nationella säkerhetsråd som Moderaterna vill etablera på Regeringskansliet för bättre ledning och samordning i cybersäkerhetsfrågorna.

15. Ge FRA och KTH i uppdrag att ta fram nya tekniska lösningar likt TDV[1] för både civilt och militärt bruk.

16. Ändra i FRA:s instruktion så att myndigheten kan stödja alla samhällsviktiga företag, inte bara statliga.

17. Utred frågan om att upprätta ett svenskt cyberhemvärn likt det som redan finns i Estland

18. Stärk samarbetet mellan den nya myndigheten för psykologiskt försvar och det nationella cybersäkerhetscentrat för att förbättra möjligheten att upptäcka och motverka påverkanskampanjer mot Sverige.

19. Initiera breda utbildningar för centralt placerade personer på svenska myndigheter och inom näringslivet för att stärka motståndskraften mot påverkanskampanjer.

20. Ge ett uppdrag till FOI att analysera hur teknologiutvecklingen påverkar framtidens påverkanskampanjer och lämna förslag på hur vi kan möta de nya utmaningarna.

21. Ta fram en strategi för ett aktivt svensk agerande inom EU för ökad energisäkerhet och för en europeisk energimarknad byggd på oberoende av rysk energi.

22. Ta fram en nationell strategi för att öka svenska företags deltagande i utvecklingsprojekt finansierade av Europeiska försvarsfonden, Europeiska försvarsbyrån och inom ramen för Pesco.

23. Utöka svenska myndigheters samarbete med det europeiska kompetenscentret för motverkande av hybridhot i Helsingfors.

24. Tydliggör i lagstiftning att energisäkerhet ska vara en viktig faktor i svensk nationell energipolitik. Leveranssäkerhet och tillgång i händelse av kris och krig måste beaktas. Vidare bör granskningssystemet för utländska direktinvesteringar göra tydligt att aktörer som är olämpliga ur säkerhetssynpunkt inte får inflytande över svensk energiproduktion.

[1] Tekniskt detekterings- och varningssystem

Bakgrund

Sverige står inför flera omfattande säkerhetshot. Ryssland har genomfört en fullskalig militär invasion av ett fredligt grannland, men invasionen är bara det senaste exemplet på Rysslands vilja att använda våld och andra typer av otillbörliga medel för att upprätthålla sin maktsfär. Dagligen ser vi exempel på ryska maktdemonstrationer som befinner sig i en gråzon mellan krig och fred. Det är detta vi kallar för hybridhot.

Såväl Försvarsmakten som Totalförsvarets forskningsinstitut har pekat på att det finns ett behov av att stärka Sveriges förmåga att möta hybridhot. Det kan handla om politiska, ekonomiska, diplomatiska eller militära påtryckningsmedel. Exempel på hybridhot kan också vara påverkanskampanjer på sociala eller traditionell media i syfte att vilseleda, eller investeringar i det privata näringslivet i syfte att uppnå geopolitiska maktmedel. Att Sverige kan värja sig också mot denna typ av hot, och har egen förmåga att motverka hoten, är av största vikt för vår säkerhet.

De senaste åren har vi sett en rad stora cyberattacker mot Sverige, liksom mot flera andra EU-länder. I början av mars i år drabbades Nordea av en så kallad överbelastningsattack och förra sommaren drabbades Coop av en attack som fick butikernas kassasystem att haverera. Gemensamt för många av denna typ av cyberangrepp är att spåren pekar mot Ryssland.

Ett belysande exempel på de pågående hybridhoten är det som skedde i Åbo skärgård 2018. Ryska, till synes privata, intressen hade under en längre tid köpt upp flera fastigheter i den finska skärgården längs strategiskt viktiga farleder. Dessa fastigheter utrustades med helikopterplattor, kajer med möjlighet att kunna ta emot större fartyg samt radarutrustning. Trots att det företag som köpt fastigheterna uppgavs arbeta med turism stod fastigheterna tomma. Dessutom sattes övervakningskameror upp och folk förbjöds att närma sig dem. Med andra ord fanns goda anledningar att anta att det bedrevs verksamhet som syftade till att undergräva finsk säkerhet. 2018 ingrep de finska myndigheterna på bred front. Hundratals personer, flera tungt beväpnade, från en lång rad finska myndigheter som Polisen, Försvarsmakten, Gränsbevakningen och Skattemyndigheten slog till samtidigt mot de ryskägda fastigheterna för att säkra bevis för olaglig och säkerhetshotande verksamhet. Detta sände en tydlig signal till både vänner och motståndare att Finland inte tolererade det som skedde och att man var beredd att slå till med kraftfulla åtgärder.

Ryssland drar sig inte heller för att använda kriminella metoder i syfte att upprätthålla sin maktsfär och skydda sina intressen utomlands. Se senaste åren har flera europeiska demokratier drabbats av dessa metoder. 2014 sprängde agenter för den ryska militära underrättelsetjänsten GRU två ammunitionslager i Tjeckien, och 2015 skadades en bulgarisk vapenhandlare och hans son svårt av ett nervgift, där spåren pekar också pekar på GRU. Ett välkänt fall ägde rum 2018 då den ryske regimkritikern Sergej Skripal och hans dotter förgiftades i Salisbury i Storbritannien. 2019 var det i stället Tysklands tur att drabbas av den ryska regimens beställningsmord när den tjetjenske separatisten Zelimchan Changosjvili sköts ihjäl i en park i Berlin. Också Sverige har drabbats av denna typ av kriminell maktutövning 2020 när en tjetjensk medborgare i Gävle utsattes för ett mordförsök. I den efterföljande rättsprocessen pekade tingsrätten på att mordet var initierat av den talmannen i den ryska delrepubliken Tjetjeniens parlament, som en blodshämnd för att offret uttalat sig kritiskt mot pappan till regimens president.

Vid sidan av Ryssland utgör i dag Iran och Kina enligt Säpo de största säkerhetshoten mot Sverige, genom en rad aktiviteter som befinner sig under hybridhotsparaplyet. Dessa tre länder bedriver spionage, och använder ekonomiska medel för att nå geopolitiskt inflytande. Inte minst när det gäller Kina har den svenska medvetenheten om hur landet använder ekonomiska investeringar för att nå

geopolitiska mål, länge varit alltför dålig. Det faktum att Sverige först 2020 avslutade ett över tio år gammalt samarbetsavtal mellan Rymdbolaget och ett bolag kopplat till kinesiska militären, om användning av en antenn vid rymdbasen Esrange, visar att vi länge varit alltför naiva i förhållande till kinesiskt ägande inom strategiskt känsliga sektorer.

Hybridhot kan också handla om att inhemska eller utländska intressen med spridning av vilseledande eller uppviglande information söker söndra den svenska demokratin. Ett exempel på detta såg vi nyligen i samband med de våldsamma upplopp som följde av planerade koranbränningar i en rad svenska städer. Polisen kunde i efterhand bekräfta att det både fanns kopplingar till kriminella nätverk till de som deltog och att det hade förekommit uppvigling från utlandet.

Moderaterna menar att Sverige aldrig ska acceptera de hot som riktas mot vårt samhälle och vår demokrati. Hela samhällets kraft måste mobiliseras för att bygga upp motståndskraft mot hybridhot, vilket spänner över en rad konkreta militära och civila förmågor. Det handlar om att kriminalisera hybridhot, om att stärka granskningen av utländska investeringar, men också om att delta aktivt i europeiska samarbeten för att utveckla nya förmågor, inte minst på cyberområdet.

Moderaternas förslag

Definiera, kriminalisera och skärp straffen för hybridhot

Hybridhoten är till sin karaktär svåra att definiera i och med att de befinner sig i en gråzon mellan krig och fred. Det ligger i angriparens intresse att agera så nära gränsen för upptäckt som möjligt för att därmed överraska och vilseleda försvararen liksom att undvika beredskapshöjning och andra motåtgärder.

Dagens lagstiftning innebär att det är svårt att lagföra personer trots att de agerat med konspirativa metoder mot svenska säkerhetsintressen. Exempelvis har den svenska strafflagstiftningen som handlat om att beivra olika former av påverkanskampanjer som syftar till att gå främmande makt tillhanda inte ändrats på snart 40 år.

Lagstiftningen måste bli tydligare när det gäller vilka gärningar som kan anses vara ett allvarligt hot mot Sveriges säkerhet och som bör definieras som hybridhot. Detta är helt nödvändigt för att brottsbekämpande myndigheter ska kunna ha ett tydligt ramverk att agera utifrån och kunna lagföra dem som bryter mot det.

Straffsatserna för brott mot rikets säkerhet är dessutom för låga. Exempelvis är straffskalan för olovlig underrättelseverksamhet mot Sverige – ett brott som täcker olika former av underrättelseverksamhet som sker med hemliga eller konspirativa metoder – fängelse i mellan 14 dagar och två år. För brottet obehörig befattning med hemlig uppgift döms inte sällan endast till böter.

- Tillsätt en utredning som har till uppgift att göra en total översyn av svensk strafflagstiftning i relation till hybridhoten. Utredningen bör bland annat lämna förslag på hur det straffbara området ska utökas för att fånga in alla relevanta hybridhot samt föreslå lämpliga straffskärpningar.

Åtgärder mot intrång, spionage och sabotage

Främmande makt har ett intresse av att verka på svenskt territorium. Det kan handla om underrättelseinhämtning, att visa närvaro för att förstärka ett hot eller om att sabotera säkerhets- och samhällsviktig verksamhet. De drönare som det har rapporterats om över svenska kärnkraftverk och andra viktiga installationer är ett aktuellt exempel.

Den traditionella underrättelseinhämtningen utgör också fortsatt ett hot mot Sveriges säkerhet, och något som ytterligare aktualiserats i och med kriget i Ukraina. Traditionella angrepp, som att stjäla information från högteknologisk industri och forskning, att försöka påverka politiska beslut eller att kartlägga skyddsobjekt, fortsätter. Under senare år har aktiviteterna från andra länder dessutom breddats. Säpo uppskattar att en tredjedel av de diplomater som verkar vid Rysslands ambassad är underrättelseagenter. Hittills har Sverige endast valt att utvisa tre av dessa, medan andra europeiska länder har utvisat betydligt fler. Sverige bör rimligtvis inte vara sämre än andra EU-länder och därför utvisa alla de ryska underrättelseagenter som verkar under diplomatisk täckmantel. Detta bör såklart ske i överensstämmelse med gällande svensk rätt och folkrättsliga regler för diplomatiska beskickningar. Vi vill också att Sverige i ljuset av Säpos kartläggning av utländsk underrättelseverksamhet tar fram en offensiv strategi för att utvisa alla, inte bara ryska, underrättelseagenter som verkar under diplomatisk täckmantel, alltså som inte är ackrediterade för underrättelseverksamhet.

Signalspaning är ett viktigt verktyg för att kunna identifiera hot mot rikets säkerhet. Idag är det dock inte tillåtet att signalspana när både sändare och mottagare befinner sig i Sverige. Det försvårar möjligheterna att använda signalspaning för att möta hybridhot där till exempel två utländska agenter kommunicerar med varandra på svensk mark. Därför behövs en översyn av två av paragraferna i signalspaningslagen som slår fast att signalspaning är helt förbjuden mellan avsändare och mottagare som båda befinner sig i Sverige.

Sverige behöver utökade verktyg som kan användas i ett gråzonsläge för att stödja Polisen och dels behöver lagstiftningen ses över så att myndigheter kan samverka och stödja varandra i ökad utsträckning. Det faktum att Försvarsmakten inte kunde stödja Polisen med gränsbevakning fullt ut under pågående den coronakrisen är ett belysande exempel på detta.

Såväl den svenska gränsen som EU:s yttre gräns måste stärkas. Under 2021 har vi sett försök av Belarus auktoritära ledare Aleksandr Lukasjenko att destabilisera EU genom att använda sig av flyktingar som hybridhot. Att Frontex nu stärks resursmässigt, liksom samarbetet mellan EU-ländernas nationella gränsbevakningsmyndigheter, är ett viktigt steg för att möta detta hot. Vi kan också konstatera att Kustbevakningen som har en central roll för att bevaka Sveriges 240 mil långa kust har fått allt fler uppgifter, men att myndighetens anslag inte har vuxit i takt med uppgifterna.

Autonoma system spelar också en allt viktigare roll på det framtida slagfältet. Sverige ligger efter på detta område och saknar till exempel effektiva system för att bekämpa drönare. Det finns också problem när det gäller lagstiftningen som omgärdar drönare. Det kan till exempel vara svårt att avgöra vad som är en otillåten flygning vid ett skyddsområde och Polisen kan inte i tillräcklig utsträckning ta hjälp av Försvarsmakten vid extraordinära händelser enligt Polisens hemställan till regeringen från 2020.

- Ta fram en offensiv strategi för att utvisa alla utländska underrättelseofficerare som verkar under diplomatisk täckmantel på svensk mark
- Ge Försvarsmakten och Polisen i uppdrag att ta fram en samlad strategi för att möta hotet från drönare samt föreslå de lag- och regelförändringar som behövs för att kunna agera resolut mot potentiella kränkningar.

- Ändra signalspaningslagen för att tillåta signalspaning även om både avsändare och mottagare befinner sig i Sverige.
- Återupprätta den särskilda beredskapspolisen för att stärka Sverige möjligheter att möta hybridhot även i fredstid.
- Ändra lagstiftningen så att Försvarsmakten ges möjlighet att stödja Polisen vid extraordinära händelser och tillse att Försvarsmakten kompenseras resursmässigt för denna nya uppgift.

Åtgärder mot otillbörliga utländska aktiviteter inom ekonomi, handel och industri

I början av digitaliseringen var det västliga demokratier som dominerade utvecklingen. Numera har dock Kina en ledande ställning inom områden som ansiktsigenkänning, 5G, kvantdatorer och digitala betalningslösningar. Även vital infrastruktur som hamnar, järnvägar, energiproduktion, satellitteknik och undervattenskablar i andra länder, inklusive Sverige, har varit föremål för kinesiska uppköp, investeringar och entreprenader. Inte sällan av statskontrollerade kinesiska bolag. Ryssland har också visat intresse för fastighetsförvärv i Sverige på platser som är intressanta ur ett säkerhetsperspektiv.

Även inom den traditionella industrin finns anledning att se över de potentiella risker som dolda ägandeförhållanden, exempelvis med inblandning av den kinesiska staten, kan innebära. I december avslöjade Göteborgs-Posten i ett granskande reportage att kinesiska staten, genom en rad dolda bolagskonstruktioner, är ägare i Geely-koncernen utvecklingsbolag Cevt, som utvecklar mjukvara för Volvo Cars självkörande bilar. Detta trots att Volvo Cars hade förnekat att statligt kinesiskt ägande fanns i koncernen. Kinesiska staten är också ägare av en undervattenskabel för datatrafik i Östersjön.

Sverige saknar ett granskningssystem för att kunna kontrollera utländska direktinvesteringar som skulle kunna hota nationella svenska säkerhetsintressen. Tack vare Moderaterna finns det nu ett utredningsförslag till hur ett sådant granskningssystem skulle kunna se ut. Det är nu viktigt att detta system kommer på plats så fort som möjligt.

På samma sätt finns sedan 2019 utredningsförslag[2] för att begränsa det kommunala självstyret i frågor av betydelse för rikets säkerhet, såsom hamnar och flygplatser. Detta genom att införa ett statligt kontrollsystem för att ytterst kunna stoppa ett köpt eller upplåtelse av exempelvis en kommunalt ägd hamn. En fråga som exempelvis uppmärksammades i samband med Karlshamns kommuns beslut att tillåta upplåtelse av en hamn för rörläggning till den ryska gasledningen Nordstream 2.

Svensk konkurrenskraft och näringsliv behöver även värnas på andra sätt. Cyberspionaget mot näringslivet ökar konstant och kostar stora mängder pengar och jobb. Den nya säkerhetsskyddslagen kommer att vara ett viktigt verktyg för att skydda information och verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot. Ett omfattande arbete kommer krävas för att implementera den nya lagstiftningen och det kommer vara resurskrävande för Säpo som bär huvudansvar för detta.

Underrättelse- och säkerhetstjänsterna har i dag inget uttalat uppdrag att stödja företag som utsätts för skadliga aktiviteter av fientliga aktörer. Det behövs därför en översyn av hur samhällsviktiga svenska företag kan få stöd för att upptäcka och motverka spionage och attacker mot sin verksamhet.

[2] SOU 2019:34 ”Förbättrat skydd för totalförsvaret”

Slutligen handlar det inte bara om yttre hot utan även hur vi själva agerar. Det gäller särskilt inom den finansiella sektorn, men även inom andra områden. Den senaste tiden har det funnits åtskilliga exempel som svenska storbanker, men även statliga bolag och institutioner, som avstår från att investera i vår försvarsindustri med hänvisning till olika policydokument. Detta slår undan fötterna på vår egen industri som är en viktig del av försvarsförmågan och gynnar de auktoritära stormakter som hotar svensk säkerhet.

- Få granskningssystemet för utländska direktinvesteringar på plats så snart som möjligt och se till att det finns en tillräcklig finansiering för att det ska fungera effektivt.
- Säkerställ att Säpo har tillräckligt med resurser för att arbeta med att utbilda och stödja svenskt näringsliv i arbetet med säkerhetsskyddslagen.
- Gör en översyn av hur samhällsviktiga företag kan få särskilt stöd av underrättelse- och säkerhetstjänsterna för att kunna upptäcka och motverka spionage och attacker mot sin verksamhet.
- Kartlägg de policydokument som statliga bolag och institutioner använder sig av och som riskerar att få negativa effekter på svensk förmåga och säkerhet.
- Begränsa det kommunala självstyret i frågor som berör nationell säkerhet genom att införa ett statligt kontrollsystem av t.ex. hamnar och flygplatser
- Kartlägg det utländska ägandet av antagonistiska stater i den svenska industrin

En stärkt cybersäkerhet

Sverige är idag ett av världens mest digitaliserade länder, men när det gäller vår cybersäkerhet är det sämre beställt. Sverige ligger först på 43 plats i världen enligt *National Cybersecurity Index*.

Sverige har redan utsatts för ett antal större cyberattacker – det gäller såväl offentlig som privat verksamhet. Kalix kommun utsattes för ett större angrepp under december 2021 och dagligvarukedjan Coop drabbades i somras. I båda dessa fall rörde det sig om utpressningsattacker där syftet är att få offret för attackerna att betala för att deras system ska kunna gå att använda igen. Även cyberspionaget ökar, här är Kina en mycket aktiv aktör.

Det finns brister såväl när det gäller ansvar och struktur som resurstilldelning och säkerhetskultur. Ansvaret för cyberfrågorna är i dag fragmenterat och uppdelat på minst fyra departement och åtta myndigheter. 2020 inrättades visserligen ett nationellt cybersäkerhetscentrum, vilket var en bra och efter frågad åtgärd. Problemet är att det inte finns något tydligt utpekat ledaransvar hos de fyra myndigheterna som har huvudansvaret för centrat.

Säkerhetsexperter har också pekat av behovet av att bygga ut utbildningsinstitutioner för att Sverige ska kunna uppnå en kompetensförsörjning på cyberområdet. Något som redan gjorts i bland annat Norge, Schweiz, Tyskland och Frankrike. Sedan 2020 finns ett centrum för cyberförsvar och informationssäkerhet vid KTH men vi skulle också behöva ett riktigt campus med nationella utbildnings- och forskningsresurser. På så sätt skulle Sverige få en kompetensbas för cyberförsvar som skulle kunna nyttjas av både det militära försvaret, civil offentlig sektor och av näringslivet.

Den svenska motståndskraften på cyberområdet skulle också förstärkas genom att upprätta ett cyberhemvärn bestående av frivilliga IT-experter, i likhet med det som redan finns i Estland och som presenterades i en rapport från Totalförsvarets forskningsinstitut 2017.

FRA utför idag ett viktigt arbete när det gäller att stödja statliga myndigheter och statligt ägda bolag med att identifiera och möta hot mot cyber- och informationssäkerheten. Ett viktigt verktyg

som FRA använder är TDV. Det är ett varningssystem som kan upptäcka avancerade IT-angrepp som normalt inte upptäcks av kommersiella antivirusskydd. FRA bör i samarbete med KTH få ett bredare uppdrag att ta fram nya verktyg, liknande TDV för användning för såväl civilt som militärt bruk. Dessutom bör FRA:s instruktion ändras så att myndigheten kan stödja alla samhällsviktiga företag, inte bara statliga sådana.

- Grunda ett nationellt cyberförsvarscampus, med egna utbildnings- och forskningsresurser, samt en ändamålsenlig budget
- Inrätta en cyberkoordinator på det nationella säkerhetsråd som Moderaterna vill etablera på Regeringskansliet för bättre ledning och samordning i cybersäkerhetsfrågorna.
- Ge FRA och KTH ett uppdrag att ta fram nya tekniska lösningar likt TDV som kan användas såväl inom cyberförsvaret som inom civil cybersäkerhet.
- Ändra i FRA:s instruktion så att myndigheten kan stödja alla samhällsviktiga företag, inte bara statliga.

Åtgärder mot desinformation och valpåverkan

Sociala medier såsom Facebook, Twitter och TikTok står ofta i centrum för diskussionen om tillförlitlighet och utländsk påverkan. Dessa plattformar är tacksamma att använda för att sprida felaktig information som snabbt får fäste. Säpo pekar också på att desinformationen under coronakrisen har ökat och att det är länder som Ryssland, Kina och Iran som ligger bakom. I dessa länder finns så kallade ”trollfabriker” som i stor skala bedriver ett informationskrig dagligen.

Framgent väntar än större utmaningar i takt med den allt snabbare teknologiutvecklingen. Ett sådant exempel är så kallade deepfakes. I korthet handlar det om att det med hjälp av avancerad artificiell intelligens går att göra förfalskade filmer med kända personers röster och ansikten som inte går att skilja från en riktig med blotta ögat. Dessa filmer kan spridas och användas för att leverera budskap som passar det egna syftet.

Informationskriget är ett viktigt vapen i samband med allmänna val. Det finns trovärdiga uppgifter att särskilt Ryssland har försökt påverka en lång rad val i länder som USA, Tyskland och Frankrike. I september är det dags för val till riksdagen, regioner och kommuner. Sverige måste stå väl rustat för att kunna identifiera och bjuda motstånd mot eventuell påverkan i samband med detta.

- Stärk samarbetet mellan den nya myndigheten för psykologiskt försvar och det nationella cybersäkerhetscentrat för att förbättra möjligheten att upptäcka och motverka påverkanskampanjer mot Sverige.
- Initiera breda utbildningar för centralt placerade personer på svenska myndigheter och inom näringslivet för att stärka motståndskraften mot påverkanskampanjer.
- Ge ett uppdrag till FOI att ta analysera hur teknologiutvecklingen påverkar framtidens påverkanskampanjer och lämna förslag på hur vi kan möta de nya utmaningarna.
- Utred frågan om att upprätta ett svenskt cyberhemvärn likt det som redan finns i Estland

Stärk det svenska deltagandet för nya försvarsförmågor på EU-nivå

För att möta hybridhoten behöver vi i högre grad satsa på innovation, både för de nutida och framtida utmaningarna. Dessvärre har maktbalansen när det gäller forskning och utveckling kraftigt förskjutits till antagonisternas favör. Både Kina och Ryssland har utvecklat sin hybridkrigföring och satsat stort på industrispionage och militär forskning.

Detta är dock något vi kan bemöta då västs civila tekniska kraft är mångdubbelt större än exempelvis Rysslands. Då krävs att vi i högre grad samordnar våra resurser och satsar på gemensamma forsknings- och utvecklingsprojekt.
Ett viktigt steg är att på EU-nivå satsa mer på forskning inom en rad hybridförmågor som tjänar hela totalförsvaret. Vi ser att Försvarets materielverk, FOI, Försvarshögskolan och Försvarsmakten alla är i behov av ökade medel och samarbeten för att möta denna hotbild. Detta skulle tjäna vår försvarsförmåga men även befolkningen i helhet då nya tjänster och innovationer kan framtas.

Sverige måste också agera inom ramen för EU och tillsammans med övriga västliga demokratier för att stärka forskning- och utveckling inom strategiskt viktiga hybridhotsområden. I dag underpresterar Sverige när det gäller att ta del av de medel som finns inom ramen för exempelvis den nystartade Europeiska försvarsfonden (EDF), som finansierar forskning på hybridhotsområdet, eller inom ramen för det permanenta strukturerade samarbetet inom EU:s försvarspolitik (Pesco). Trots en välutvecklad försvarsindustri deltar vi inte i något Pesco- eller EDF-projekt på exempelvis cyberområdet. Nederländerna, men också Norge, har redan tagit fram strategier för hur deras respektive länders försvarsindustrisektorer ska ta del av medlen i EDF. Sverige borde följa detta exempel och omedelbart ge försvarsdepartementet i uppdrag att ta fram en liknande strategi för att öka det svenska deltagandet i EDF och Pesco. Fokus bör här särskilt ligga på finansiering av nya förmågor, exempelvis de som ryms inom hybridhotsbegreppet såsom cyber- och rymdförmåga.

Därtill bör Sverige genom relevanta myndigheter utöka sitt samarbete med det europeiska kompetenscentrum för motverkande av hybridhot som sedan 2017 finns baserat i Helsingfors.

- Ta fram en nationell strategi för att öka svenska företags deltagande i utvecklingsprojekt finansierade av Europeiska försvarsfonden, Europeiska försvarsbyrån och inom ramen för Pesco.
- Utöka svenska myndigheters samarbete med det europeiska kompetenscentret för motverkande av hybridhot i Helsingfors.

Stärk Europas energisäkerhet

Byggandet av de ryska gasledningarna Nord Stream 2 (NS2) mellan Ryssland och Tyskland har varit i fokus för diskussionen om energi och säkerhet de senaste åren. Gasledningen har nu stoppats av Tyskland till följd av Rysslands invasion i Ukraina, men Europas beroende av rysk gas består. Att vissa länder i EU är så beroende av rysk gas att ett EU-embargo mot rysk gas förblir en praktisk omöjlighet är en svaghet som måste åtgärdas genom stärkt energioberoende.

Också i Sverige ser vi hybridhot på energiområdet, trots vår mycket begränsade import av rysk energi. Den nedstängning av kärnkraften som sker i Sverige och ökade satsningar på alternativa energislag drar till sig intresse från Kina. China General Nuclear Power Group är ett statsägt kinesiskt bolag. Redan idag är man via ett dotterbolag delägare i sex svenska vindkraftsparker. Det ställer frågor om hur det kinesiska ägandet skulle kunna användas som politiskt maktmedel vid en eventuell ekonomisk eller politisk konflikt med Sverige eller EU. Av detta skäl är det viktigt att bygga ut det svenska granskningssystemet av utländska direktinvesteringar i energisystemet för att på så sätt kunna stoppa investeringar som skapar politiska risker.

De skenande elpriser vi har sett i Sverige under vintern understryker problemet med ett energisystem som inte kan ha en stark leveranssäkerhet oavsett årstid eller väder. Avvecklingen av den svenska kärnkraften är därför mycket olycklig ur ett säkerhetsperspektiv och gör oss sårbara för

påverkan utifrån. På europeisk nivå har kärnkraftens betydelse för energisäkerhet och oberoende lyfts fram för att på sikt möjliggöra en utfasning av rysk gas.

- Sverige ska vara en tydlig röst inom EU för ökad energisäkerhet och för en europeisk energimarknad byggd på oberoende av rysk energi.
- Energisäkerhet ska vara en viktig faktor i svensk nationell energipolitik. Leveranssäkerhet och tillgång i händelse av kris och krig måste beaktas.
- Det måste vara tydligt i granskningssystemet för utländska direktinvesteringar att aktörer som är olämpliga ur säkerhetssynpunkt inte får inflytande över svensk energiproduktion.