Välkomna till Försvarsmaktens
digitala lägesuppdatering.

Vid min sida står Daniel Olsson-

-ställföreträdande chef för Militära
underrättelse- och säkerhetstjänsten, Must-

-men också Patrik Ahlgren,
chef för Försvarsmaktens cybersektion.

Vi kommer prata om Försvarsmaktens bild
av det som sker i Ukraina-

-och hur det påverkar den säkerhetspolitiska
utvecklingen i Sveriges närområde.

Därefter kommer Patrik Ahlgren fördjupa sig
i cyberförsvaret och vikten av det.

Därefter öppnar vi upp för frågor.

Först lämnar jag över ordet
till Daniel Olsson. Varsågod.

Tack, och god eftermiddag.

Jag representerar den militära underrättelse-
och säkerhetstjänsten, Must-

-en civil och en militär underrättelsetjänst.

Vi följer alltså civila och militära hot och är
dessutom Sveriges militära säkerhetstjänst.

Must är en del av Försvarsmakten-

-men har två uppdragsgivare:
regeringen och överbefälhavaren.

Vårt uppdrag är att stödja svensk utrikes-,
säkerhets- och försvarspolitik.

Vi ska kartlägga yttre hot mot Sverige,
oavsett hur och var de kommer till uttryck.

Och vi ska motverka säkerhetshot
som riktas mot Försvarsmakten.

Jag ska dela med mig av några
av de övergripande bedömningar-

-som Must gör en dryg månad efter att
Ryssland inledde sitt anfallskrig mot Ukraina.

Jag ska också ge några kommentarer
om det aktuella läget i Ukraina.

Jag kommer att undvika
att gå in på enskildheter-

-mot bakgrund av den höga sekretessen
inom underrättelse- och säkerhetstjänsten.

Låt mig först säga
att Rysslands anfall 24 februari-

-inte kom som en blixt från klar himmel.

Rysslands agerande under en längre tid
har orsakat ett försämrat säkerhetsläge-

-i Europa som helhet
och i Sveriges närområde.

Vi har länge sett en utveckling
mot en allt hårdare rysk maktpolitik-

-på bekostnad av regelbaserade
ordningar, rustningskontroll-

-multilateralt samarbete,
folkrätt och demokrati.

Ryssland har försökt att omkullkasta den
existerande europeiska säkerhetsordningen-

-som byggdes på grundval av erfarenheterna
av andra världskriget och kalla kriget-

-och i stället få ett erkännande
för en privilegierad intressesfär-

-och en buffertzon i sitt närområde-

-som då skulle begränsa suveräniteten och självbestämmanderätten för Rysslands grannländer.

Ryssland har länge haft
en låg tröskel för militär våldsanvändning-

-särskilt mot länder i sitt nära utland.

Det har man visat i krigen i Georgien 2008,
i Ukraina sedan 2014 och i Syrien sedan 2017-

-liksom med agerandet av
så kallade privata militära firmor-

-i Syrien, Libyen, den Centralafrikanska
republiken och nu senast i Mali.

Utvecklingen mot en större europeisk kris
har alltså pågått under en längre tid.

Den accelererade under senhösten och vintern-

-med den ryska styrkeuppbyggnaden
vid Ukrainas gräns - som Must kunde följa nära -

-och med de ytterst långtgående ryska krav
på en radikalt ny säkerhetsordning i Europa.

Vad kan Must då idag dra för övergripande
slutsatser av Rysslands anfall på Ukraina?

Den mest grundläggande slutsatsen är att
det säkerhetspolitiska läget har försämrats.

Det gäller i Europa som helhet
och i Sveriges närområde-

-dit vi räknar Östersjöregionen,
Barents hav och Nordatlanten.

Vi bedömer också att Ryssland
- från en redan tidigare låg nivå som jag nämnde -

-ytterligare har sänkt sin tröskel
för att använda militärt våld.

Invasionen av Ukraina visar
att den ryska statsledningen är beredd-

-att ta mycket stora risker, både militärt
och politiskt, för att uppnå sina mål.

Större risker än man tidigare tagit.

Det är tydligt att Ryssland
har underskattat Ukrainas motståndskraft.

Det gäller såväl militärt
som politiskt och i hela samhället.

Ryssland har på ett liknande sätt underskattat
västs sammanhållning och beslutsamhet-

-vilja att stödja Ukraina och förmåga
att försvaga rysk ekonomi med sanktioner.

Det ingick inte heller i den ryska
kalkylen att flera europeiska länder-

-skulle göra långtgående förändringar
av sin säkerhets- och försvarspolitik-

-där Tysklands beslut att snabbt öka
sina försvarsutgifter till två procent av BNP-

- det motsvarar idag
drygt 700 miljarder kronor per år -

-är den förändring
som får störst betydelse på sikt.

Mot den här bakgrunden
bedömer Must att Ryssland sannolikt-

-har gjort en strategisk felbedömning
med invasionen av Ukraina.

Vi kan inte utesluta
att den kan följas av fler felbedömningar.

Det finns idag en osäkerhet
om Rysslands beredskap till risktagande-

-både mot Ukraina och mot väst-

-i ett nytt läge då man är pressad
av att inte ha uppnått sina mål i Ukraina-

-av trycket av de ekonomiska sanktionerna
och av ett potentiellt missnöje i Ryssland.

Därtill har risken i detta spända läge
ökat för militära incidenter-

-som oavsiktligt skulle kunna leda
till en eskalation mellan Ryssland och väst.

Det gäller även i svenskt närområde.

Vi ser alltså ett stort utfallsrum
när vi analyserar följderna-

-för europeisk säkerhet av kriget i Ukraina.

Osäkerheten är stor för alla aktörer
i detta nya och fortsatt föränderliga läge.

Musts entydiga bedömning är att de allvarliga
spänningarna i Europa kommer att bli bestående.

Det vi ser som mest troligt är
nån form av västlig containment av Ryssland.

Det vill säga en politik som är långsiktigt inriktad
på att förhindra ytterligare expansion-

-av rysk makt och inflytande på en rad områden:

Territoriellt och militärt, men även politiskt
och ekonomiskt, och till exempel på energiområdet.

Säkerhetsläget i Europa går alltså i riktning
mot förhållanden som påminner om dem-

-som var rådande före 1989,
men troligen med färre spelregler-

-och mindre förutsägbarhet än vad
som var fallet under huvuddelen av kalla kriget.

Jag vill också säga några ord
om den militära utvecklingen i Ukraina.

Jag vill först understryka att det fortsatt
pågår ett brutalt ryskt angreppskrig-

-med strider i samtliga områden
där de ryska väpnade styrkorna är insatta.

Det var ryska uttalanden om att en ominriktning
ska ske mot Donbass och södra Ukraina-

-men vi har hittills inte sett tydliga
förändringar på marken i den riktningen.

I norra och östra Ukraina har situationen
under den senaste veckan varit statisk.

Ryska styrkor har till del avancerat i södra
Ukraina och stärkt positionerna vid Mariupol.

Ukrainska förband har genomfört
motanfall i områdena kring Kiev.

Den ryska krigföringen har fortsatt
i hög grad inriktad mot större städer.

Beskjutningen med tungt artilleri
mot dessa är urskillningslös-

-och utan hänsyn till civila offer.

Vi kan se att man i Mariupol undviker
att skada hamnen och järnvägen-

-som båda är av strategiskt
intresse för Ryssland-

-medan man skjuter mot sjukvårdsinrättningar,
livsmedelsförsörjning och skolor.

Den ryska försvarsmakten har begränsningar
vad gäller underhåll och förnödenheter-

-till sina stridande förband i Ukraina.

Man har fått betydande förluster
både av personal och materiel.

Nu förbereder eller genomför man
åtgärder som handlar om underhåll-

-samt förstärkning
och omorganisering av de insatta förbanden.

Sammanfattningsvis har Ryssland ännu inte,
efter en månad, nått sina strategiska mål-

-och det verkar inte som att de kommer kunna
nå ett militärt avgörande i Ukraina som helhet.

Försvarsmakten har inte gjort
några förändringar av bedömningen-

-av det militära hotet
mot Sverige sedan förra veckan.

Patrik Ahlgren kommer nu
att prata om cyber-

-en domän där Sverige är utsatt för intrång
och påverkansförsök dagligen.

Tack. Vi får dagligen information
om krigets händelseförlopp i Ukraina.

En artikel i Washington Post beskrev
att det har varit avgörande för Ukraina-

-att de haft tillgång
till ett fungerande internet.

Det har gjort att människorna
som är kvar i landet-

-har kunnat kommunicera
med omvärlden under kriget och om kriget.

Sedan 2015 har Ukraina arbetat långsiktigt
med att bygga upp sitt cyberförsvar.

Däri ligger bland annat att skapa förmågan att skydda
och upprätthålla viktiga samhällsfunktioner.

Ukrainska experter förutspådde tidigt
att utvecklingen av modern krigföring-

-först skulle ske
och göra avtryck i cyberdomänen.

Cybervapen är ett militärt
maktmedel som kan användas-

-för att påverka och förstöra militära
och samhällsviktiga funktioner.

Därför krävs ett starkt cyberförsvar.

Sverige är ett av världens
mest digitaliserade länder-

-och en ledande nation
på flera områden kring innovation-

-och utveckling av nya digitala lösningar.

Våra samhällstjänster har blivit
mer tillgängliga för medborgarna-

-och möjligheterna har blivit större
för att såväl konsumera information-

-som att ge uttryck för tankar och åsikter.

Detta är i många avseenden fantastiskt
och något vi ska vara stolta över.

Den enskildes uppkopplade
vardag har blivit alltmer påtaglig.

Viktiga samhällstjänster är ofta bara
några knapptryckningar bort i allas telefoner.

Sverige är i dag beroende
av kontinuerligt fungerande-

-informations- och kommunikationsteknik för
att upprätthålla viktiga samhällsfunktioner.

Sektorer som energi- och
vattenförsörjning, transporter, sjukvård-

-och livsmedelsförsörjning är
genom sina informations- och styrsystem-

-en del av det som måste kunna försvaras.

De system som vi alla är beroende av
levereras och förvaltas av företag-

-med utveckling i en mängd olika länder.

Möjligheterna för en motståndare att påverka
kritiska delar av samhällets infrastruktur-

-blir därmed fler, hoten blir svårare
att upptäcka, och riskerna blir mer svårbedömda.

Ett exempel är intrånget
mot Coops kassasystem-

-där den mest naturliga sak som
att handla mat till middag inte gick att göra.

Det var i och för sig inte Coops
betalningssystem som var målet för angriparen.

Målet var företaget
som tillverkar programvaran-

-i betalsystemet som Coop använder.

Därigenom drabbades svenska konsumenter.

Vår slutsats är att samhällskritiska
funktioner måste ha alternativa lösningar.

I Coops fall behövdes det
ett alternativt betalsystem.

De hot som finns mot samhället idag
omfattar allt från hackare-

-som av ren prestige vill ta sig in i system-

-kriminella som via internet utpressar
enskilda och företag för att tjäna pengar-

-och stater eller statsunderstödda aktörer
som satsar stora resurser-

-på att kunna genomföra storskaliga,
systempåverkande och uthålliga cyberangrepp.

Angrepp som syftar till
att tillgodose det egna landets intressen.

Vår huvuduppgift är att försvara
Sverige mot ett väpnat angrepp.

Försvarsmakten ska ha förmåga att värna
Sveriges suveräna rättigheter och intressen-

-samt att förebygga och hantera konflikter
och krig, såväl nationellt som internationellt.

Detta inkluderar även cyberdomänen.

Cyberförsvar är en integrerad del
i det militära försvaret.

Försvarsmakten upprätthåller detta genom
en förmåga att aktivt skydda egna intressen-

-och, tillsammans med andra myndigheter såsom
Försvarets radioanstalt, Säkerhetspolisen-

-och Myndigheten för samhällsskydd
och beredskap, agera proaktivt-

-för att upptäcka, få information om
och hantera cyberattacker.

Cyberförsvaret ska kunna
genomföra alla typer av operationer-

-mot andra staters väpnade styrkor
i och genom cyberdomänen.

Cyberförsvaret utformas för att
försvara egna system och funktioner-

-såväl som de tjänster
och system utanför myndigheten-

-som behövs för att möta ett väpnat
angrepp eller genomföra mobilisering.

Försvarsmakten ska kunna
verka i alla konfliktnivåer.

Men cyberförsvarets dimensionerade uppgift
är att kunna verka i höjd beredskap och krig.

Försvarsmakten ska kunna förstärka skyddet-

-av kritiska samhällsfunktioner
i krig, såväl som i fred.

Försvarsmakten startade utvecklingen
av cyberförsvaret på 00-talet-

-bland annat genom organiseringen
av ett it-försvarsförband.

Jag vill betona att Försvarsmakten
idag har de förmågor som krävs-

-och arbetar nu vidare
för att möta framtidens utmaningar.

Det vi gör nu, likt Ukraina, är
att stärka vår uthållighet och kapacitet-

-för att skapa förutsättningar för ett cyber-
försvar som ska kunna möta framtidens hotbild-

-där cyberförsvar betraktas som en självklar
förmåga och integrerad del i modern krigföring.

Vår målsättning är att bygga
ett cyberförsvar i världsklass.

Det är ett långsiktigt åtagande
med flera samverkande komponenter.

Just nu fokuserar vi på att stärka
ledningen av cyberoperationer-

-på militärstrategisk,
operativ och taktisk nivå.

Vi arbetar också med att etablera ytterligare
ett it-försvarsförband, och på sikt ett tredje.

Vi utvecklar också vår samverkan
med prioriterade internationella aktörer-

-och arbetar med att upprätta ett personal-
och karriärsystem inom cyberförsvarsområdet-

-med cybersoldater, specialistofficerare,
taktiska officerare och civila experter.

Därutöver inriktar vi forskning
och omsätter den i teknik- och metodutveckling-

-tillsammans med KTH:s centrum
för cyberförsvar- och informationssäkerhet-

-och i det arbetet deltar
flera andra svenska aktörer.

När det gäller samverkan
med andra nationella aktörer-

-har det Nationella
cybersäkerhetscentret en viktig roll.

I centret träffas de viktigaste
myndigheterna inom området-

-för att dela information
och analysera den aktuella situationen.

Detta bidrar till en gemensam lägesbild-

-som stöder och förbättrar
respektive myndighets förmåga att agera.

En viktig del i uppbyggnaden
av det svenska cyberförsvaret är att öva-

-och utmana den personal som fyller
en funktion inom Sveriges cyberförsvar.

Här vill jag framhålla
två exempel på det.

Det första är Försvarsmaktens årligen
återkommande övning, Safe Cyber-

-där vi övar olika samhällsviktiga aktörer.

2021 övade vi
luftfarts- och sjöfartssektorn.

2022 kommer vi att öva
telekomföretag och internetleverantörer.

Det andra exemplet är multinationella
övningen Locked Shields-

-som arrangeras av Natos Center
of Excellence för cyberförsvar i Tallinn.

Försvarsmakten samordnar
det svenska deltagandet i övningen-

-och i år deltar myndigheter och företag
viktiga för Sveriges energiförsörjning.

Regeringen, liksom Försvarsberedningen-

-understryker vikten av
förebyggande säkerhetsarbete-

-och att öka medvetenheten såväl som förmågan
hos alla användare av it-system-

-för att skapa förutsättningar för utvecklingen
av en säkerhetskultur i hela samhället.

Det finns brister i skyddet
för känslig svensk information-

-och det finns en förmåga i omvärlden
att komma över känslig information.

Cybersäkerhet kan inte bara lösas
på central nivå - här har vi all ett ansvar.

En viktig förutsättning för cyberförsvaret
är att alla användare av it-system-

-tar sitt ansvar för att upprätthålla
en god cybersäkerhet.

Jag vill understryka att Försvarsmakten
har ett tydligt fokus på cyberförsvar-

-och vi fortsätter att lösa våra uppgifter
så att Sverige kan vara tryggt och säkert-

-idag, imorgon och framåt. Tack.

Tack så mycket för det, både för
era beskrivningar och era fördjupningar.

Då ska vi öppna upp för frågor.
Först ut har vi TV4.

Tack. Min fråga är främst till Daniel Olsson.

Nyheterna kunde i går berätta
att källor uppger att de ryska plan-

-som kränkte svensk luftrum
över Gotland var kärnvapenbestyckade.

Kan Must bekräfta de här uppgifterna?

Försvarsmakten kommenterar
aldrig beväpning-

-på utländska stridsflygplan nära vårt luftrum.

Jag vill vara glasklar med
att det inte finns något med kränkningen 2 mars-

-som innebär en ökad hotbild mot Sverige
eller som ger skäl till ökad oro.

Vi har en mycket säker bild
av det här, en god lägesbild-

-när det gäller närområdet,
vilket inkluderar luftrummet.

Om vi hade sett att det fanns skäl
att öka bedömningen av hotet mot Sverige-

-med anledning av incidenten,
eller av andra skäl, hade vi berättat det.

Du talar om en god bild.

Utöver bilderna Försvarsmakten
delat med sig av från kränkningen-

-kunde ni även se planens
bestyckning och undersida-

-tydligare än den bild ni delat?

Jag kan inte gå in och kommentera
beväpning på utländska stridsflygplan-

-för om vi gör det över tid
så röjer vi förmågorna som vi har-

-att gå ut med de uppgifterna,
och det vill vi inte bjuda på.

Jag förstår. Tack.

Tack för det, TV4. Vi släpper in
Göteborgs-Posten. Varsågod.

Tack! Jag har en fråga om cyberattacker.

Hur mycket cyberattacker
utsätts Sverige för nu i fredstid?

Jag kan säga något om det.

Cyberhotet är en viktig del
av den samlade hotbilden mot Sverige-

-och det som karakteriserar
den delen av hot är att det finns-

-i fred, i kris och i krig.

Det riktas mot alla delar av samhället,
oavsett om det är privat, militärt eller civilt-

-vilket gör det speciellt
och det kräver breda insatser.

När det gäller hotbilden,
de senaste veckorna har vi inte fått in-

-några anmälningar om större
angrepp mot svensk it-infrastruktur.

Vi har haft ett antal
överbelastningsattacker-

-som ryms inom det vi kallar en "normalbild".

Vi ser också tecken på att det kommer
fler anmälningar till myndigheterna-

-om att företag eller andra myndigheter
har utsatts för it-angrepp-

-vilket är viktigt för att få
en samlad lägesbild.

Det välkomnar vi förstås.

Tack.

Tack så mycket!
Då släpper vi fram DN. Varsågod.

Vi hör inte dig.

-Hör ni mig nu?
-Nu funkar det bättre.

Jag har egentligen två frågor till Must-

-om de här kränkningarna,
2 mars utanför Gotland.

De första uppgifterna sade
att de ryska planen var obeväpnade-

-men sen kom TV4 i går med uppgifter
om att de var beväpnade med kärnvapen-

-men en expert säger
att han inte ser vapen på planen.

Finns inga vapen, så finns inga detaljer
att kommentera, så frågan är:

Fanns det vapen eller inte på planen-

-oavsett om det var kärnvapen eller
konventionella vapen eller inga vapen alls.

Om det inte fanns några vapen alls,
så kan ni ju säga det.

Vi kommenterar inte beväpningsfrågor,
oavsett vilken typ av beväpning-

-när det gäller utländska stridsflygplan
i Sveriges närområde.

Det kan över tid röja vår förmåga.

Kan det vara en del
av en rysk påverkansoperation?

Vi går som sagt inte in på frågan
om beväpningen flygplanen hade-

-men vi justerar inte hotbildsbedömningen
mot Sverige, och ser inget ökat hot-

-med anledning av kränkningen.

Kan det vara en fråga om
att uppgifterna sprids från rysk sida-

-som en del av en påverkans-
operation mot Sverige?

Ja, rent generellt är det viktigt att vara
medveten om att kärnvapen kan användas-

-som psykologisk påverkan
- ett sätt att markera och skrämmas-

-när man kommer ut med uppgifter
om kärnvapen, oavsett hur.

Det är väldigt viktigt att vara
medveten om det, att hålla huvudet kallt-

-när man ser denna sortens uppgifter,
och att vara mycket källkritisk.

Det kan man säga även
i det här fallet, alltså?

En generell kommentar,
som gäller allmänt.

En till fråga om Ukraina.

Brittiska chefen för signalspanings-
organisationen höll tal i Australien i går-

-och sade om rysk krigföring
precis det som Must har sagt om bristerna-

-men dessutom säger han att kommando-
och kontrollsystemen är i kaos.

Är det också en svensk observation?

Jag skulle inte använda det ordvalet-

-men instämmer i att det verkar
finnas brister även på det området.

Tack. Får jag möjlighet att ställa
en fråga till Patrik Ahlgren också?

Varsågod, ställ din fråga.

Ukraina utsätts mycket för cyberattacker-

-och före kriget vädjade de
om stöd på cyberområdet.

Ger Försvarsmakten stöd till
Ukraina och deras cyberförsvar?

Nej.

-Varför inte?
-Vi har inte fått den uppgiften.

-Okej. Tack.
-Tack så mycket.

Då släpper vi in TT. Varsågod.

Tack. En fråga till Must.

Hur har cyberhotet specifikt
från Ryssland förändrats-

-sedan de inledde
anfallskriget mot Ukraina?

Som jag sa har vi inte sett eller fått
anmälningar om några större angrepp-

-på svensk it-infrastruktur
de senaste veckorna-

-vilket gäller efter angreppet
på Ukraina 24 februari.

Vi har sett ett antal
överbelastningsattacker-

-men det ryms inom det
vi skulle kalla en normalbild.

Slutsatsen är att vi inte ser
en ökad aktivitet i nuläget från rysk-

-eller någon annan aktörs sida.

Tack. De här överbelastnings-
attackerna som har observerats-

-kommer det från ryskt håll?

Det är väl olika...
Det är olika attacker vi pratar om.

Jag kan inte ge en samlad bild av det.

Det tillhör bilden, att attackerna
ofta kan komma från privata aktörer-

-och det är svårt att reda ut
hur kopplingen eventuellt-

-kan vara till en statlig aktör.

Har ni sett något om de här attackerna-

-om de liksom hör ihop,
om det kan handla om...?

Ja, om det handlar om enskilda attacker,
eller någon form av rekognosering-

-att man testar sig fram?

Jag vill inte gå in på
detaljer, men vi ser inte-

-att det är en samlad attack,
de här överbelastningsincidenterna.

Tack. En sista fråga:

Vilken beredskap bör enskilda
företag och privatpersoner ha?

Vad ska man vara beredd på, när det gäller
just cyberhot och cyberattacker?

Man bör naturligtvis,
som alltid, se till att man-

-har sina it-system uppdaterade
med de senaste säkerhetsuppgraderingarna.

Man bör också påminna sina medarbetarna
att vara vaksamma mot-

-de vanligaste metoderna för attacker -
phising-mejl, konstiga länkar-

-och man bör vara uppmärksam på det.

En tredje sak man kan göra är att se över
gamla konton, radera gamla konton-

-om det är medarbetare som slutat.

Låt inte deras behörigheter ligga kvar osv,
- vanlig cyberhygien, alltså.

På msb.se finns allmänna
rekommendationer för allmänheten.

Tack så mycket.

Tack så mycket från TT.

Där sätter vi punkt
för dagens digitala lägesuppdatering.

Tack så mycket för
att ni varit med oss! Hej då!