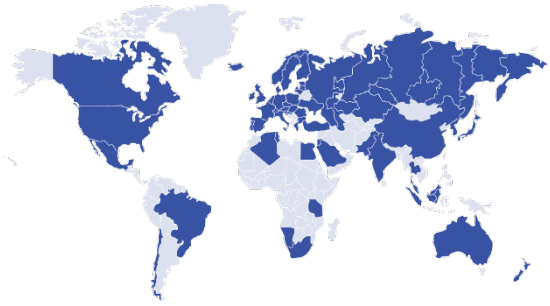
# Årliga rapporter

Flera svenska myndigheter och internationella organisationer rapporterar årligen information om hoten, möjligheterna och utmaningarna på cyberområdet. Rapporterna visar en trend där antalet cyberattacker ökar och allt fler attacker utförs av statliga eller statsunderstödda aktörer.



*Militära Underrättelse- och säkerhetstjänstens* årsöversikt ger inblick i myndighetens verksamhet och presenterar en översikt av Sveriges och omvärldens militära och säkerhetspolitiska utveckling. Bland annat lyfts att den snabba teknikutvecklingen skapar en mer komplex hotbild på cyberområdet, vilket kräver en stärkt offentlig/privat samverkan. 25 februari 2021.

*Säkerhetspolisens* årsbok presenterar hoten mot Sverige hur och olika stater bedriver underrättelse gentemot Sverige, där Kina, Ryssland och Iran anges vara de länder som utgör det allvarligaste hotet. Om främmande makt kommer över svensk forskning och innovation bedöms det kunna få stora konsekvenser för svensk tillväxt. 18 mars 2021.

*FRA* framhäver i sin årsrapport att cyberattacker från statliga angripare är synnerligen genomtänkta och välkoordinerade. Hotbilden anges vara både bredare och mer komplex än tidigare. Vidare påpekas att allt går att hacka sig in så länge det finns tid, resurser och kompetens. 15 mars 2021.

*Myndigheten för Samhällsskydd och beredskap (MSB)* presenterar en sammanställning och analys av de statliga myndigheternas it-incidentrapportering. Vad som sker, varför det sker och vad som ska göras för att undvika att det sker igen. Februari 2021.

*Myndigheten för Samhällsskydd och beredskap (MSB)* presenterar en årsrapport med en samlad bild över NIS-leverantörers it-incidentrapportering 2020. Rapporteringen visar att incidenter ofta sker i tjänst som tillhandahålls av underleverantör och att bristfälliga kontrakt kan leda till informations-brist gällande incidenterna. Totalt rapporterades 88 incidenter 2020 vilket är en ökning från 2019. Dock anges att en mycket liten del av incidenterna har orsakats av angrepp. 5 februari 2021.

*Samverkansgruppen för informationssäkerhet (Samfi)* har presenterat 2021 års redovisning av den samlade informations- och cybersäkerhetshandlingsplanen. Mars 2020

I *World Economic forums* 16e version av den Globala rapporten presenteras de risker som väntas under året. Cyberattacker bedöms som ett av de största hoten samhällen står inför under de kommande tio åren. 19 januari 2021.

*Munich Security Report* presenterar en översikt över stora säkerhetspolitiska utmaningar och innehåller insiktsfulla data och analyser över utvalda geografiska och tematiska områden, ett område som berörs är teknologisk nationell suveränitet. 14 februari 2020

*European Union Agency for Cybersecurity (ENISA)* presenterar i denna rapport en överblick över hoten på cyberområdet. De 15 största hoten listas följt av en djupare analys om hoten och rekommendationer om hur olika aktörer kan arbeta för att möta hoten.

# Fördjupning om cyberhoten

Cyberhoten är många och tar sig uttryck på flera olika sätt. Några aktuella hot rör industrispionage, forskningssamarbete, företagsförvärv och 5G. Läs mer om dessa och flera hot nedan.


## Industrispionage

*Information Technological and Innovation Foundation (ITIF)* diskuterar den kinesiska statens stöd till kinesiska teknologiska bolag och ger förslag på hur omvärlden kan reagera mot kinesisk merkantilism. 22 juni 2020.

*FOI* rapporterar om Kinas cyberspionage riktat mot industri och innovationer. 22 mars 2019

*Norska säkerhetspolisens* hotbedömning anger att spionage utgör ett allvarligt hot mot Norge. Vidare anges att teknikföretag med forskningsmiljöer som arbetar med rymdbaserade tjänster, maritim teknik, hälsa och försvarsindustrin är särskilt utsatta för spionage från främmande makt. Februari 2021.

I denna artikel presenterar *Foreign Policy* industrispionaget ur ett historiskt perspektiv. Artikeln tar sin början år 500 f.k. och avslutar 2019. 27 april 2019.

*PwC* redovisar i denna rapport statsunderstött industrispionage kopplat till Cloud Hopper. April 2017

## Forskningssamarbete

*ASPI* analyserar den kinesiska militärens ökande forskningssamarbete med utländska universitet. Artikeln presenterar hoten med sådant samarbete och rekommenderar åtgärder som universitet och stater bör vidta för att säkerställa att forskning inte sprids till militära motståndare. 30 oktober 2018.

## Företagsförvärv

*FOI* kartlägger kinesiska företagsförvärv av svenska företag och presenterar strategier och planer bakom förvärven. 28 november 2019.

## Särskilt om 5G

Tankesmedjan *RUSI* framhäver risker med utvecklingen av 5G och presenterar en strategi för hur de riskerna kan hanteras. Februari 2020.

I en artikel från *Tech Republic* presenteras hot med utvecklingen av 5G i relation till sakernas internet. Det lyfts ett behov av reglering av marknaden för sakernas internet och starka proaktiva åtgärder för att säkerställa säkra 5G-nätverk. 2 mars 2020.

## Cyberhot mot rymdbaserade tjänster

*FOI* presenterar i denna rapport en omvärldsanalys av rymdområdet med fokus på säkerhet och försvar. Bland annat lyfts hotet om cyberkrigföring mot rymdbaserade tjänster. Vidare analyseras hur USA och Kina arbetar med cyberfrågor kopplade till rymden. Januari 2021.

## Hoten i leveranskedjorna

*FOI* undersöker i denna studie vad cyberleveranskedjor är och vilka hotbilder som finns mot dessa. Syftet med studien är att förmedla kunskap gällande de risker som kan uppstå i cyberleveranskedjor och vad som går att göra för att motverka dessa risker. 2 december 2019

## Digitaliseringstekniker

*USA:s National Counterintelligence and Security Center* identifierar nya risker med disruptiva tekniker (cyber), inte minst möjligheterna de erbjuder aktörer med mindre resurser att orsaka stor skada. 22 januari 2019

*FOI* tar utgångspunkt i digitaliseringens komplexitet och några av de förändringsparadigm som digitaliseringen medför och sammanfattar de huvudsakliga problem som Sverige måste hantera för att möjliggöra en ändamålsenlig digitalisering inom offentlig förvaltning. 11 februari 2020

## Cyberhoten under pandemin

*Finska Skyddspolisen* ger i denna rapport en överblick av den nationella säkerheten 2020. I den anges bl.a. att pandemin medfört att cyberspionage riktas mot två nya sektorer: läkemedelsindustrin och forskningsinstitutet. Det anges också att det är sannolikt att auktoritära stater försöker utnyttja den pågående pandemin och att den nationella säkerheten äventyras om tillgången till information ges företräde framför alla andra komponenter av informationssäkerhet i nyckelsystem.

*Europol* ger en översikt över hur brottslingar har anpassat sina attacker under pågående pandemi då allt fler har tvingats förlita sig på digitala lösningar. Det framkommer att, även om brottslingar i grunden använder samma metoder som innan pandemin, är de duktiga på att ändra narrativet till pågående pandemi för att nå ökad framgång. 11 november 2020.

## Omvärldsbevakning

*FOI* presenterar i denna slutrapport ett projekt om cyberoperationer som utförts mellan 2017-2020 åt Försvarsmakten. Fokus ligger därför på Försvarsmaktens behov av ökad förmåga att utföra cyberoperationer. December 2020. I anslutning till rapporten presenteras även en omvärldsbevakning av statsattribuerade cyberoperationer 2020. 18 december 2020.

*Norwegian Institute of International Affairs* granskar offensiv militär cyberförmåga ur ett småstatsperspektiv med utgångspunkt i Norge och Nederländerna för att nyansera den så ofta amerikanskt dominerade debatten. 12 mars 2019

*Estonian Foreign Intelligence Service* analyserar de externa säkerhetspolitiska hoten mot Estland och i 2021 års rapport framställs Ryssland som det fortsatt största hotet mot västerländska demokratier. Metoderna som använts tidigare används fortfarande och angreppen bedöms fortsätta att öka. 17 februari 2021.

*FOI* analyserar utformningen och implementeringen av den ryska cyberstrategin 2000-2020. 26 oktober 2020.

*Estlands International Centre for Defence and Security* jämför den militära cyberorganisationen i fem europeiska länder (Estland, Finland, Tyskland, Nederländerna och Norge) under rubriken Preparing for Cyber Conflict. December 2018

*Forskare vid University of Nottingham* lyfter i en artikel begreppen ”Cyber sovereignty” och ”Cyber hegemony” med utgångspunkt i kinesisk politik. 7 september 2018

# Cyberhoten i siffror

Hur många cyberangrepp sker det egentligen? Hur många av dem drabbar Sverige? Hur drabbat är Sverige och svenska företag jämfört med andra länder? Nedan hänvisas till information som ger en bättre förståelse för omfattningen av cyberattackerna.

*Center for Strategic and International Studies (CSIS)* sammanställer signifikanta cyberincidenter sedan året 2006.

*Estlands* The National Cyber Security Index är ett globalt index som mäter beredskapen från länder för att förhindra cyberhot och hantera cyberincidenter. Sverige placerar sig 2021 på plats nummer 42 av 160 undersökta länder. År 2020 placerade sig Sverige på plats nummer 41.

*PwC* presenterar i en rapport att åtta av tio svenska bolag menar att de har varit utsatta för cyberincidenter under det senaste året, och att svenska företag är mest utsatta jämfört med företag i de andra nordiska länderna. 20 februari 2020

# Kostnaderna som följer av cyberattacker

En konsekvens av cyberattacker är ekonomisk förlust. Hur stora summor går förlorade varje år? Vad är kostnaden för att skydda sig från cyberattacker? Hur mycket kan företagen vinna på att arbeta preventivt mot cyberattacker? SOFF har samlat länkar som kan ge dig svar på dessa frågor.

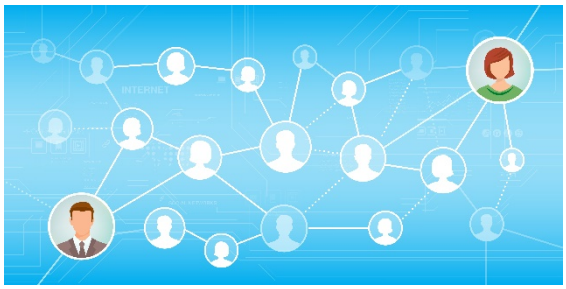
*Norwegian Institute of International Affairs* analyserar i **en rapport** hur en eventuell cyberattack på norska olje- och gasleveranser skulle få både ekonomiska och säkerhetspolitiska konsekvenser för större del av Europa. 23 februari 2018

*Mcafee* redovisar kostnaderna för cyberattacker och drar slutsatsen att 946 miljarder dollar, strax över en procent av den globala BNP, går förlorade varje år. Det är en ökning med 346 miljarder dollar sedan 2018. Rapporten framhäver förutom ren ekonomisk förlust också flera dolda kostnader som kan uppstå som direkta eller indirekta konsekvenser av angreppen. December 2020.

*Ponemon* och *Accenture* redovisar kostnaden för cyberattacker för företag – och kostnaden för att skydda sig. 2019.

# Preventivt arbete och utvärdering av cyberhoten

Genom att arbeta preventivt kan antalet cyberattacker och skadorna till följd av cyberattacker minimeras. Men vad kan egentligen göras för att förebygga konflikter och skada av eventuella angrepp?



*EUs institut för säkerhetsstudier* presenterar en sammanfattning av dagens metoder och framtida möjligheter till förebyggande åtgärder i relation till konflikter i cyberspace. 17 april 2020.

Det amerikanska underrättelseorganet för signalspaning, *National Security Agency (NSA)* sammanfattar och utvärderar cyberarbetet år 2020. Bland annat redogörs för NSAs arbete med kryptografi och cybersäkerhet för telenät. 8 januari 2021.

*Brittiska cybersäkerhetscentret (NCSC)* har presenterat CyBok, slutversionen av den den guide till cybersäkerhetsarbete som bl.a. ger vägledning för utformning av utbildningar och kunskapsutveckling. 31 oktober 2019

*MSB* presenterar i denna rapport en uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Rapporten förklarar vad det innebär att arbeta systematiskt med informationssäkerhet och presenterar en uppföljningsstruktur för att utvärdera arbetet och ger förslag på vidareutveckling av uppföljningsstrukturen. 1 mars 2021.

I en artikel i tidningen *Forbes* ges förslag på hur cybersäkerhet kan förklaras för de med mindre teknisk sakkunskap. Dessutom ges tips på hur företag kan arbeta med och utvärdera cybersäkerheten i företaget. 15 maj 2020.

*FOI* utforskar i denna rapport möjligheterna av att utnyttja artificiell intelligens (AI) inom ett dataangrepps olika faser. Rapporten lyfter olika fall som påvisar scenarion av AI mot mänsklig teknikanvändare och AI mot teknik där den senare även omfattar aspekter av en kapprustning mellan AI-stödd angripare och AI-stödd försvarare. 30 mars 2020

# Svenskt nationellt cybersäkerhetscenter

I december 2020 fattade regeringen beslut om att ge Försvarets radioanstalt (FRA), Försvarsmakten och Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag att inrätta ett nationellt cybersäkerhetscenter. Centret är tänkt att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot.


---

*FRA, Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen* presenterar i denna slutrapport förslag för att tillsammans vidta förberedande åtgärder för att ett svenskt nationellt cybersäkerhetscenter ska kunna inrättas under 2020. 16 december 2019

I denna rapport från FMV, FRA, Försvarsmakten, MSB, Polisen, PTS och SÄPO redogörs närmre för cyberhoten och hotaktörerna. Bland annat redogörs för vilka som är de största hotaktörerna och vilka deras drivkrafter är. Rapporten går också igenom olika metoder för initial åtkomst till det angripna systemet. Vidare diskuteras mer strukturella brister och beroenden som påverkar den svenska cybersäkerheten idag och hur Sverige bör arbeta med cybersäkerhet framöver. 3 juni 2020.

I denna rapport från FMV, FRA, Försvarsmakten, MSB, Polisen, PTS och SÄPO rekommenderas säkerhetsåtgärder för att möta cyberhoten. 3 juni 2020.

# Regelverk på cyberområdet

Den ökade närvaron och de ökande hoten i cyberrymden innebär allt fler lagar och regler som svenska staten och svenska företag måste förhålla sig till. Vad ställer GDPR och NIS-direktivet för krav på företag? Hur måste företag arbeta med juridisk informations-säkerhet? Behövs det fler regler?

*EU:s revisorer* varnar för flera utmaningar inom EU:s cybersäkerhet. Rapporten illustrerar initiativ och förklarar bl.a. skillnaden mellan GDPR och NIS-direktivet mycket pedagogiskt. Mars 2019

Idag är de flesta överens om att internationell rätt ska appliceras på cyberattacker. Frågan kvarstår närmre hur internationell rätt ska appliceras. Tallinn Manualen 2.0 är framtagen av en expertgrupp och kan fungera som vägledning för hur internationell rätt kan appliceras på cyberarenan.

*The Wired* tar upp frågan om det behövs ett internationellt regelverk för cyberkrig, om det är genomförbart eller är det alltför tid- och resurskrävande? Artikeln pekar på ett flertal faktorer och lyfter framtida utmaningar. 21 februari 2018

*Kommerskollegium* presenterar **en rapport** om hur brist på internationell samordning av regler för IT-säkerhet hindrar utvecklingen samt kopplingen till internationell handel. 11 juni 2018

*Advokatbyrån Kahn Pedersen* har tagit fram en rapport om "juridisk informationssäkerhet" vilken går igenom svenska regelverk. 12 mars 2020

*Advokatbyrån Kahn Pedersen* har tagit fram en rapport om ”publika molntjänster” som bland annat redogör för särskilda överväganden som gäller för verksamheter som omfattas av säkerhetsskyddslagen och NIS-lagen. Senast uppdaterad 18 november 2020.

*MSB* presenterar i skriften "Så skapar vi motståndskraft" som underlag till försvarsbeslutsperioden 2021-2025. Skriften tar bl.a. tar upp genomförandet av Försvarsberedningens förslag inom cyber- och totalförsvar. 28 februari 2020

*Regeringen* presenterar i denna utredning ett förslag till en struktur för ansvar, ledning och samordning inom civilt försvar. Bland annat föreslår utredningen att cybersäkerhet ska vara särskilt beredskapsområde. Februari 2021.