Myndigheten
för civilt försvar

Cyberangreppens utveckling 2023–2025

Årsrapport cyberincidentrapportering 2025

**Cyberangreppens utveckling 2023–2025 –
Årsrapport cyberincidentrapportering 2025**

Myndigheten för civilt försvar
651 81 Karlstad

Enhet: Enheten för strategisk cybersäkerhet

Foto: Melker Dahlstrand (omslag), Pavel Koubek (sida 8)
Johan Eklund (sida 12), Mikael Svensson (sida 14),
Cultura Creative (sida 34), Icon Photography (sida 58, 62)
Tryck: Ljungbergs Tryckeri AB
Produktion: Advant

Publikationsnummer: MCF0108 – mars 2026
ISBN-nummer: 978-91-7927-731-4

Förord

Sverige befinner sig i ett allvarligt säkerhetspolitiskt läge. Samtidigt fortsätter digitaliseringen av samhällets alla sektorer i rasande fart. Det erbjuder möjligheter, men det skapar också sårbarheter. Cyberdomänen spelar en central roll i krigsföring, och cyberangreppen utvecklas kontinuerligt. Det ställer krav på samhället att snabbt stärka motståndskraften i samhällsviktiga informationssystem.

Därför är det efterlängtat att den nya cybersäkerhetslagen är på plats, vilket innebär en omfattande ambitionshöjning för cybersäkerhetsarbetet i hela Sverige och EU. Lagen innebär att långt fler verksamhetsutövare omfattas av rapporteringsplikt vid inträffade cyberincidenter. En utökad rapporteringsplikt är välkommen eftersom myndigheten bedömer att det fortsatt föreligger ett stort mörkertal i incidentrapporteringen. Mörkertalet hämmar myndighetens arbete med att sammanställa en heltäckande nulägesbild och att ta fram det stöd som krävs för att förebygga och hantera de svåraste problemen på cyberområdet.

I årets temakapitel fördjupar vi oss i cyberangreppens utveckling mellan 2023 och 2025. Andelen cyberangrepp som förekommer i incidentrapporterna 2025 har minskat. Samtidigt har myndigheten noterat allvarliga angrepp mot ot-system de senaste åren, däribland angrepp mot ot-system hos våra skandinaviska grannländer. Därför är det viktigt att organisationer jobbar systematiskt med att identifiera både interna och externa risker och hot, exempelvis genom att följa upp incidenter och bevaka händelser i omvärlden.

Samlat visar årets rapport på vikten av att fortsätta arbetet med att stärka Sveriges civila försvar och beredskap inom cybersäkerhet. Jag ser även fram emot att Myndigheten för civilt försvar den 1 juli lämnar över stafettpinnen i cyberfrågorna till Nationellt cybersäkerhetscenter under ledning av Försvarets radioanstalt. Tillsammans hjälps vi åt att öka Sveriges samlade motståndskraft.

Stockholm, 26 mars 2026

Åke Holmgren
Avdelningschef, avdelningen för cybersäkerhet
och samhällsviktiga kommunikationer

Innehåll

Centrala ord och uttryck 6

Sammanfattning 9

Om rapporten 13

Rapporterade cyberincidenter under 2025 15

Om cyberincidentrapportering 15

Inkomna cyberincidentrapporter 16

- Organisationer som har rapporterat in incidenter 2025 16
- Flest incidentrapporter från hälso- och sjukvårdssektorn 17
- Störst andel incidentrapporter från offentlig förvaltning 19
- Bristande rapporteringsbenägenhet 20
- Minskning av inrapporterade leverantörsincidenter 21
- Misstag och systemfel fortsatt de vanligaste orsakerna 22
- Andelen cyberangrepp i incidentrapporterna har minskat 24
- Cyberincidenter uppstår ofta i it-miljön 26
- Cyberincidenterna påverkar ofta informationssystemens tillgänglighet 29

Tema: Cyberangreppens utveckling under 2023–2025 35

Oklart om totalt antal cyberangrepp globalt har ökat eller minskat 36

- Flera rapporterar om ökat antal angrepp mot Ukraina och Ukrainas allierade 37
- Metod som räknar cyberangrepp visar ett minskat antal sedan 2023 39

AI har möjliggjort effektivisering av cyberangrepp 41

- Användningen av AI ökar och effektiviserar cyberangrepp enligt företag och vissa myndigheter 42
- AI har skapat möjlighet för fler aktörer att utföra angrepp och utöva digitalt försvar 43

Överbelastningsangrepp har blivit mer avancerade och ökat i flera avseenden 44

- Överbelastningsangrepp har ökat i flera avseenden 44
- Överbelastningsangrepp har blivit mer komplexa 46

Angrepp mot digitala leveranskedjor kan ha ökat i vissa avseenden 46
Angrepp mot digitala leveranskedjor kan ha ökat från låg nivå 47
Fysiska komponenter kan påverka digitala leveranskedjor 48
Indikationer på att antalet angrepp mot ot-system har ökat 49
Flera rapporterar om en ökning av antalet angrepp mot ot-system 50
Flera europeiska länder drabbade av angrepp mot ot-system 51
Angrepp mot ot-system med koppling till geopolitik 52
Cyberangrepp kan vara ett medel för cyberspionage och informationspåverkan 52
Cyberspionage är ett hot inom och utanför cyberkrigföring 53
Cyberangrepp är ett verktyg för informationspåverkan 54
Cyberangrepp används mer i samband med kinetiska angrepp i cyberkrigföringen 55

Slutsatser och rekommendationer 59
Hotaktörer utvecklar kontinuerligt sin cyberangreppsförmåga 59
Incidentrapporteringen måste förbättras 60
Många angrepp har en koppling till geopolitik 61

Framåtblick 63

Centrala ord och uttryck

I detta kapitel förklaras rapportens centrala begrepp och akronymer.

Allriskperspektiv: Att sträva efter att bedöma alla typer av risker oavsett om de uppstår i fredstid eller vid höjd beredskap.

CERT: En förkortning för ”Computer Emergency Response Team”. En funktion med uppgift att stödja samhället i arbetet med att hantera och förebygga cyberincidenter.

CSIRT: En förkortning för ”Computer Security Incident Response Teams”. CSIRT-nätverket, som etablerades genom NIS-direktivet (EU) 2016/1148, är ett nätverk av nationellt utpekade CERT-funktioner för hantering av cyberincidenter. Myndigheten för civilt försvar/CERT-SE är Sveriges nationella CSIRT.

Cyberangrepp: Angrepp, via cyberrymden, som är specifikt riktad mot en nation, organisation eller annan aktörs användning av cyberrymden med avsikten att förstöra, inaktivera eller ta över kontrollen över ett datasystem.

Cyberoperation: En operation via cyberrymden i syfte att påverka en intern eller extern infrastruktur.

Cybersäkerhet: Ett samlingsnamn för informations-, it, ot- och leveranskedjesäkerhet. Informationssäkerhet handlar om åtgärder för att skydda informations tillgänglighet, riktighet och konfidentialitet. It- och ot-säkerhet är i sin tur de tekniska åtgärder som vidtas inom digitala miljöer för att säkra informationstillgångar respektive funktioner. Leveranskedjesäkerhet handlar om att säkerställa säkerhet i system och tjänster som en annan organisation tillhandahåller till en organisation.

Cybersäkerhetslagen: Den svenska anpassningen av EU:s NIS2-direktiv (2022/2555). NIS2-direktivet behandlar åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen.

Digital leveranskedja: De tjänster och infrastrukturer som levererar eller möjliggör leverans av digitala produkter och används för att upprätta, upprätthålla, utveckla eller återställa en verksamhets informationshantering och informationssystem.

ECCC: En förkortning för ”European Cybersecurity Competence Centre”. EU:s kompetenscentrum för cybersäkerhet vars uppdrag är att främja europeisk innovation och industripolitik inom informations- och cybersäkerhetsområdet.

Enisa: Europeiska unionens byrå för nät- och informationssäkerhet, ”European Union Agency for Network and Information Security”.

Incident: En inträffad oönskad händelse. Vid incidentrapportering delas orsaker bakom incidenter in enligt mänskliga hot (både antagonistiska hot i form av angrepp och icke-antagonistiska hot i form av misstag), tekniska hot (i form av systemfel) eller naturhot (såsom väderfenomen, jordbävningar med mera).

Informationssystem: System för att samla in, lagra, bearbeta och distribuera information för ett givet ändamål.

IoT: En förkortning för begreppet ”Internet of Things” som används för att beskriva att allt fler föremål, både för privat- och industriellt bruk, utrustas med möjligheten att anslutas till internet och andra nätverk.

Konfidentialitet: Egenskap hos informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

Monoberoende: En organisation har ett monoberoende av (exempelvis) en tjänst när den är beroende av den tjänsten och det inte finns några alternativa tjänster att använda ifall den tjänst man redan använder upphör.

NIS-leverantör: Leverantörer av samhällsviktiga och digitala tjänster som omfattas av NIS-regleringen.

NIS-regleringen: Samlingsnamn på den lag (SFS 2018:1174), förordning (SFS 2018:1175) och de föreskrifter som antagits i Sverige för att implementera NIS-direktivet (EU) 2016/1148.

Ot-system: System för operativ teknik, ot-system, lagrar och bearbetar information samt reglerar fysiska styrsystem, ofta med direkt påverkan på människa eller omgivning. Det kan till exempel handla om styrsystem för kollektivtrafik, produktion av kraftvärme, dricksvattensystem och skyddsdörrar.

RCDC: Förkortning för ”The Regional Cyber Defence Centre” som är en cybersäkerhetsorganisation under Litauens Nationella cybersäkerhetscenter.

Riktighet: Egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring.

Störning: En konsekvens av en incident som innebär att en samhällsviktig eller digital tjänst inte kan tillhandahållas på avsett sätt.

Tillgänglighet: Egenskap hos informationstillgång som innebär att den är åtkomlig och användbar inom förväntad tid och omfattning

Överbelastningsangrepp: Angreppsmetod som bygger på att stora mängder datatrafik skickas mot en server eller annan nätverkskomponent i syfte att begränsa dess förmåga att bearbeta data och därmed blockera åtkomst för annan, legitim datatrafik. Datatrafiken kan skickas från en, ett fåtal, respektive ett stort antal av angriparen kontrollerade enheter. I det senare fallet brukar angreppet benämnas som ett ”DDoS-angrepp” (”Denial of service”, ”Distributed denial of service”).

Sammanfattning

Sammanfattning

Andelen inrapporterade angrepp till Myndigheten för civilt försvar har fortsatt att minska, men samtidigt har vissa typer av cyberangrepp ökat under vissa perioder.

Medan årsrapportens temakapitel redogör för att vissa typer av cyberangrepp har ökat under åren 2023–2025, har andelen inrapporterade angrepp till myndigheten minskat under 2025. Majoriteten av de inrapporterade incidentrapporterna har angett ”okänd” som orsak, följt av ”misstag” eller ”systemfel”. Däremot visar myndighetens analys att majoriteten av de okända incidenterna oftast kan härledas till systemfel.

Antalet inkomna cyberincidentrapporter har fortsatt att minska. Under 2025 har totalt 266 cyberincidenter rapporterats till Myndigheten för civilt försvar från 95 unika organisationer. 122 rapporter har inkommit från statliga myndigheter och 144 från leverantörer av samhällsviktiga och digitala tjänster, NIS-leverantörer. År 2024 inkom 319 cyberincidentrapporter från 163 unika organisationer. Medan inrapporteringen från NIS-leverantörer har varit relativt oförändrad de senaste tre åren, har inrapporteringen från statliga myndigheter minskat. Majoriteten av de cyberincidentrapporter som inkommit från NIS-leverantörer består liksom tidigare år av organisationer inom hälso- och sjukvårdssektorn (80 procent), följt av dricksvatten- (13 procent) och transportsektorn (4 procent). Andelen cyberangrepp har minskat 2025 jämfört med tidigare år.

Rapportens temakapitel visar att hotaktörer kontinuerligt utvecklar sin cyberangreppsförmåga, tillämpar flera olika angreppsmetoder, och angriper olika sektorer. Exempelvis har källorna som myndigheten analyserat redogjort för att angrepp mot ot-system har ökat under perioden 2023–2025, och likaså överbelastningsangrepp mot statliga aktörer. Temakapitlet visar att många angrepp har en koppling till geopolitik. Samtidigt har vissa metoder blivit mer avancerade med hjälp av AI, och vissa överbelastningsangrepp har blivit mer omfattande och svårhanterliga. Kapitlet redogör också för utvecklingen av cyberangrepp som medel för spionage och informationspåverkan, och att cyberangrepp har använts alltmer i kombination med kinetiska angrepp i krigföring.

Mot bakgrund av denna utveckling lämnar Myndigheten för civilt försvar ett antal rekommendationer till samhällsviktiga verksamhetsutövare.

Rekommendationer

- Utveckla, prioritera och resurssätt det systematiska och riskbaserade cybersäkerhetsarbetet.
- Använd Myndigheten för civilt försvars och Nationellt cybersäkerhetscenters stöd och verktyg för att utveckla cybersäkerhetsarbetet, samt följ myndigheternas rekommendationer för hur verksamheter kan förebygga och hantera olika angrepp.[1]
- Stärk arbetssätten för incidentrapportering för att få en bättre förståelse för varför incidenter drabbar den egna verksamheten och bidra till Sveriges motståndskraft.
- Bedriv omvärldsbevakning för att identifiera risker, som hot och sårbarheter.[2]

Not 1. Se lista över Myndigheten för civilt försvars tillgängliga stöd och verktyg i Myndigheten för samhällsskydd och beredskap, *Verktyg för ökad motståndskraft och stärkt civilt försvar*, 2025.

Not 2. Omvärldsbevakningen bör samla information från leverantörer av organisationens hårdvara och mjukvara, Sveriges nationella CSIRT, expert- och tillsynsmyndigheter samt källor som bevakar den övergripande utvecklingen av ny teknik på it-området.

Om rapporten

Om rapporten

Den här rapporten är framtagen på uppdrag av regeringen i enlighet med Myndigheten för civilt försvars instruktion[3] och riktar sig till beslutsfattare, cybersäkerhetsansvariga, samt omvärldsbevakande och analyserande funktioner hos samhällsviktiga verksamhetsutövare.

Rapportens kapitel om cyberincidentrapportering avser att informera om cybersäkerheten hos svenska organisationer, vilka incidenter som sker, orsakerna till dem och konsekvenserna de medför. Detta kapitel redogör för de cyberincidentrapporter som inkom till Myndigheten för civilt försvar under 2025, och som således har rapporterats in under den lagstiftning som gällde under 2025.

Årets temakapitel redogör för utvecklingen av cyberangrepp inom ett urval av områden för åren 2023–2025. Det handlar om antal cyberangrepp, utvecklingen av överbelastningsangrepp, användning av AI inom cyberangrepp, cyberangrepp mot leveranskedjor, cyberangrepp mot ot-system och utvecklingen av cyberangrepp inom cyberkrigföring i ljuset av kriget i Ukraina. Syftet med temakapitlet är att ge samhällsviktiga verksamhetsutövare en bild av hur delar av cybersäkerhetslandskapet ser ut idag, vilka cyberhot Sverige kan stå inför och vilka åtgärder som krävs för att stärka cybersäkerheten, öka motståndskraften och förebygga eller förhindra att cyberincidenter uppstår.

Not 3. Sveriges Riksdag. Förordning (2008:1002) med instruktion för Myndigheten för civilt försvar.

Rapporterade cyberincidenter under 2025

Rapporterade cyberincidenter under 2025

Verksamheter som är viktiga för det svenska samhällets funktionalitet ska rapportera om cyberincidenter som drabbat dem till Myndigheten för civilt försvar. Detta kapitel redogör för de inrapporterade incidenterna under 2025.

Om cyberincidentrapportering

Det är viktigt att rapportera cyberincidenter. Ju mer information som tillhandahålls kring incidenter, desto bättre kan det systematiska cybersäkerhetsarbetet utvecklas och struktureras. Att incidentrapportera är att stötta svenska samhällsviktiga verksamhetsutövare och samhället i stort. Incidentdata bidrar även till Myndigheten för civilt försvars analyser som ligger till grund för de metodstöd och verktyg som myndigheten tar fram.

Vissa organisationer har krav på sig att rapportera incidenter eftersom den verksamhet de bedriver anses särskilt kritisk för samhällets funktionalitet. De organisationer som under 2025 hade krav på sig att rapportera cyberincidenter till Myndigheten för civilt försvar är statliga myndigheter under regeringen och leverantörer av samhällsviktiga och digitala tjänster (NIS-leverantörer).[4] Från 2026 kommer en ny portal för cyberincidentrapportering att öppna, i samband med att föreskrifterna till cybersäkerhetslagen har trätt i kraft. Portalen kommer att erbjuda nya lösningar för de rapporteringspliktiga organisationer som omfattas av cybersäkerhetslagen.

Under särskilda omständigheter kan en och samma cyberincident behöva rapporteras till flera olika myndigheter. Om en incident innefattar påverkan på personuppgifter är den rapporteringspliktig enligt dataskyddsförordningen (GDPR) och ska, utöver rapportering till Myndigheten för civilt försvar, rapporteras till Integritetsskyddsmyndigheten. En incident som faller under rapporteringsskyldigheten enligt säkerhetsskyddsförordningen ska rapporteras till Säkerhetspolisen eller Försvarsmakten. Myndigheten för civilt försvar uppmanar

Not 4. Sveriges riksdag, Förordning (2022:524) om statliga myndigheters beredskap; Sveriges riksdag, Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

alla organisationer att proaktivt se över vilka rapporteringskrav som gäller för olika typer av cyberincidenter för att kunna agera snabbt och korrekt om och när en incident inträffar.

Inkomna cyberincidentrapporter

Under 2025 mottog Myndigheten för civilt försvar totalt 266 cyberincident-rapporter från rapporteringspliktiga organisationer. Utav dessa inkom 122 rapporter från 41 statliga myndigheter och 144 från 54 NIS-leverantörer,[5] se tabell 1. Det utgör en minskning i jämförelse med tidigare år. Minskningen följer samma trend som de senaste åren då statliga myndigheter inkommit med allt färre cyberincidentrapporter.

Tabell 1. Antalet inkomna cyberincidentrapporter 2022–2025

Rapporteringskrav	2025	2024	2023	2022
Statliga myndigheter	122	170	189	231
NIS-leverantörer	144	149	144	99
Total	**266**	**319**	**333**	**330**

Organisationer som har rapporterat in incidenter 2025

Sammantaget har 95 rapporteringspliktiga organisationer inkommit med minst en cyberincidentrapport. Av dessa har 54 rapporterat i enlighet med NIS-förordningens rapporteringskrav och 41 i enlighet med statliga myndigheters rapporteringskrav. Detta utgör en väsentlig minskning i förhållande till föregående år då totalt 163 unika organisationer inkom med minst en cyberincidentrapport. Det är således en minoritet av de rapporteringspliktiga organisationerna som inkommer med en cyberincidentrapport. År 2025 inkom 16 procent av alla rapporteringspliktiga statliga myndigheter[6] med minst en cyberincidentrapport. Motsvarande andel bland NIS-leverantörer uppskattas vara nio procent.[7]

Enskilda statliga myndigheter och NIS-leverantörer står för en större del av samtliga inkomna cyberincidentrapporter. Ungefär en tredjedel av incident-rapporterna som inkommit i enlighet med statliga myndigheters rapporterings-krav har kommit från en och samma myndighet, och ungefär en tredjedel av

Not 5. Med statliga myndigheter menas de statliga myndigheter under regeringen som är rapporteringspliktiga enligt förordningen (2022:524) om statliga myndig-heters beredskap, beredskapsförordningen. Vissa statliga myndigheter är istället rapporteringspliktiga enligt NIS-förordningen. NIS-leverantörer avser samhälls-viktiga och digitala tjänster och innefattar till exempel vissa statliga myndigheter, offentliga organisationer och privata företag.

Not 6. Rapporteringsplikten omfattar alla statliga förvaltningsmyndigheter under regeringen, AP-fonder, Domstolsverket och statliga affärsverk. Utlandsmyndigheter omfattas av Utrikesdepartementets rapporteringsplikt, och Sveriges domstolar omfattas av Domstolsverkets.

Not 7. Myndigheten för civilt försvar har inte exakt data på antalet NIS-leverantörer. Beräkningar bygger därför på en uppskattning.

incidentrapporterna i enlighet med NIS-lagstiftningens rapporteringskrav har inkommit från två rapportörer, som båda är regioner. Sammantaget står offentlig sektor för nästan samtliga inkomna incidentrapporter, trots att Myndigheten för civilt försvar uppskattar att privata företag utgör majoriteten av rapporteringspliktiga NIS-leverantörer.

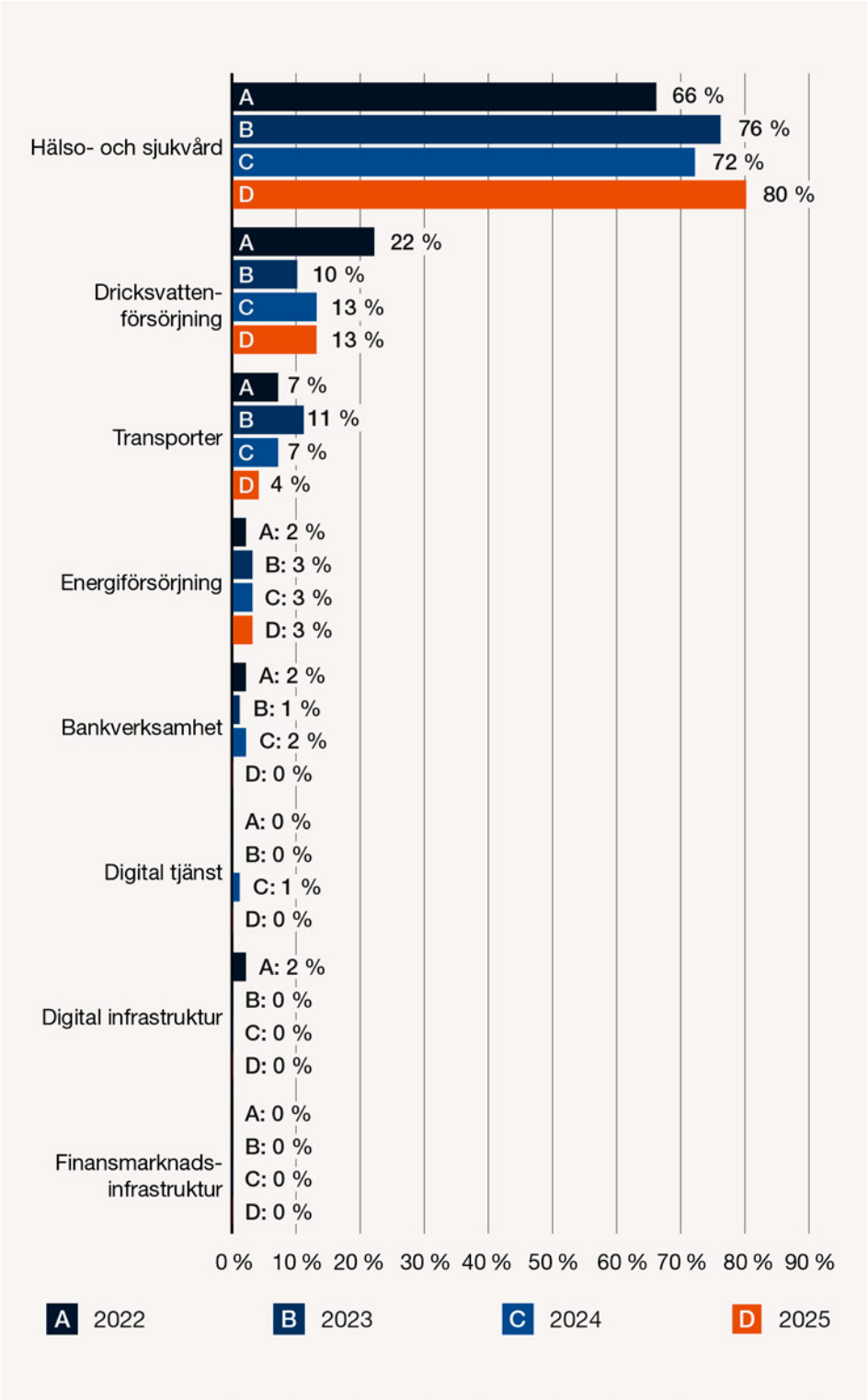
Givet de fortsatt svaga resultaten för offentlig förvaltning i 2025 års Cybersäkerhetskollen, ett verktyg som bedömer svenska organisationers cybersäkerhetsarbete, har myndigheten inte skäl att tro att den minskade rapporteringen beror på förbättringar i det systematiska cybersäkerhetsarbetet eller att färre incidenter inträffar till följd av ett förbättrat förebyggande arbete.[8]

Flest incidentrapporter från hälso- och sjukvårdssektorn

Som **diagram 1** åskådliggör har 80 procent av de cyberincidentrapporter som inkommit från NIS-leverantörer rapporterats av organisationer inom hälso- och sjukvårdssektorn. Andelen utgör en ökning jämfört med föregående år, men sett till absoluta termer är det en minskning i antalet cyberincidentrapporter totalt. Dricksvatten- och transportsektorn stod för 13 respektive fyra procent av rapporterade cyberincidenter, medan energiförsörjningen stod för tre procent. Resterande sektorer har inkommit med enstaka eller inga cyberincidentrapporter alls under det gångna året.

Not 8. Myndigheten för civilt försvar, *Cybersäkerhetskollen 2025 Redovisning av uppföljning av nivån på det systematiska cybersäkerhetsarbetet i offentlig förvaltning och samhällsviktig verksamhet*, 2026.

Diagram 1. Andel cyberincidentrapporter per NIS-sektor 2023–2025



Att den offentliga hälso- och sjukvårdssektorn är överrepresenterad bland NIS-leverantörer bedöms bero på flera faktorer. En huvudsaklig anledning kan vara att majoriteten av NIS-leverantörer som inkommer med incidentrapporter

är kommuner och regioner, i kombination med att kommuner och regioner framförallt är rapporteringspliktiga som leverantörer av samhällsviktiga tjänster inom hälso- och sjukvård.[9]

Störst andel incidentrapporter från offentlig förvaltning

Den stora merparten av de cyberincidentrapporter som inkommit i enlighet med NIS-lagen har rapporterats av organisationer inom offentlig förvaltning. Därtill uppskattas ytterligare 22 procent ha rapporterats av kommunala bolag. Andelen privata företag som rapporterar incidenter har sjunkit ytterligare från 25 procent 2024 till totalt 15 procent 2025. Fördelningen illustreras i **diagram 2**.

Diagram 2. Fördelningen av unika rapporterande NIS-leverantörer baserat på aktörsgrupp 2025

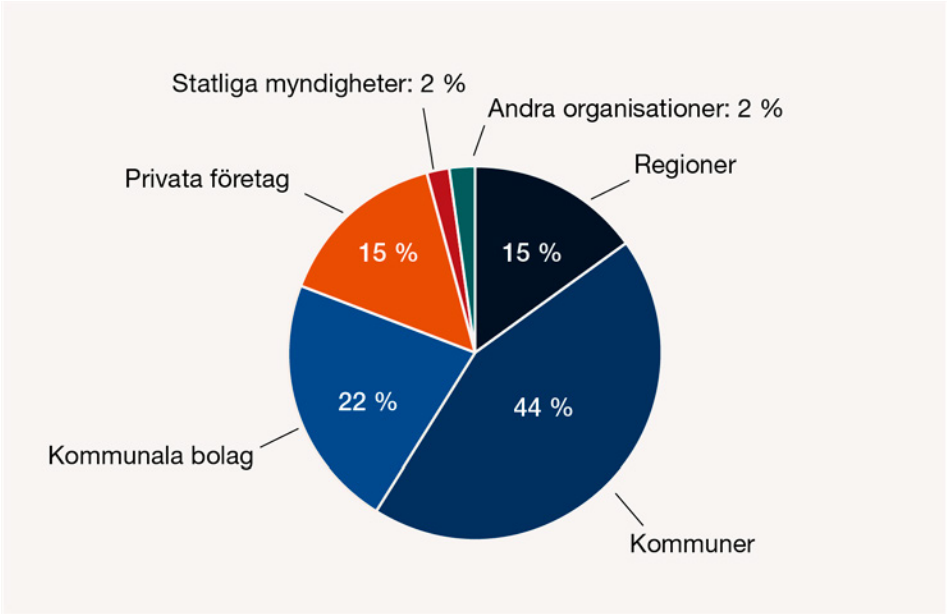
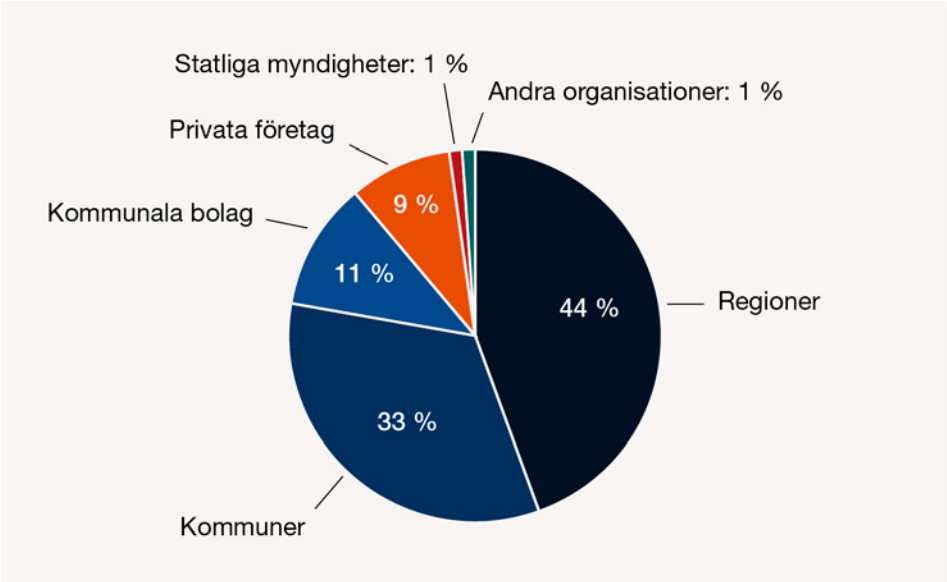


Diagram 3 visar andelen cyberincidentrapporter totalt som inkommit från respektive aktörsgrupp i enlighet med NIS-förordningen. Noterbart har cirka 44 procent av cyberincidentrapporterna inkommit från Sveriges regioner, och 33 procent från kommunerna. Det behöver inte innebära att flertalet cyberincidenter sker inom region- och kommunsektorn, men det visar att regioner och kommuner är mer benägna att inkomma med cyberincidentrapporter. Generellt har Myndigheten för civilt försvar observerat att offentliga förvaltningar, så som kommuner och regioner, är mer benägna att respektera rapporteringsplikten än andra organisationer. Den stora merparten av cyberincidentrapporter som inkommer från regioner och kommuner beskriver störningar inom regional eller kommunal hälso- och sjukvård.

Not 9. Se kriterier som gör en cyberincident rapporteringspliktig i enlighet med Myndigheten för civilt försvars föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9).

Diagram 3. Fördelningen av inkomna cyberincidentrapporter av NIS-leverantörer per aktörsgrupp 2025



Bristande rapporteringsbenägenhet

Myndigheten för civilt försvar har länge gjort bedömningen att det förekommer ett större mörkertal i cyberincidentrapporteringen, både inom ramen för NIS-leverantörers och statliga myndigheters rapporteringskrav.

I de inkomna incidentrapporterna för år 2025 framkommer att vissa organisationer har högre rapporteringsbenägenhet än andra. Dessa organisationer rapporterar en stor variation av incidenter, såväl avbrott med måttlig påverkan som långvariga störningar med betydande påverkan. Det är osannolikt att denna stora variation av incidenter endast drabbar några organisationer och inte andra. Därtill förekommer att de beskrivna störningarna är av en sådan typ som berör flera organisationer, men att Myndigheten för civilt försvar endast har fått in incidentrapporter från ett fåtal verksamhetsutövare. Ett stort antal rapporteringspliktiga organisationer har dessutom aldrig inkommit med en enda incidentrapport. Av de statliga myndigheter som var rapporteringspliktiga under 2025 har 28 procent inte rapporterat någon cyberincident sedan 2018, från det året Myndigheten har tillgängliga data. Slutsatsen av detta är att det 2025 fortfarande förekommer ett stort mörkertal avseende incidentrapporter.

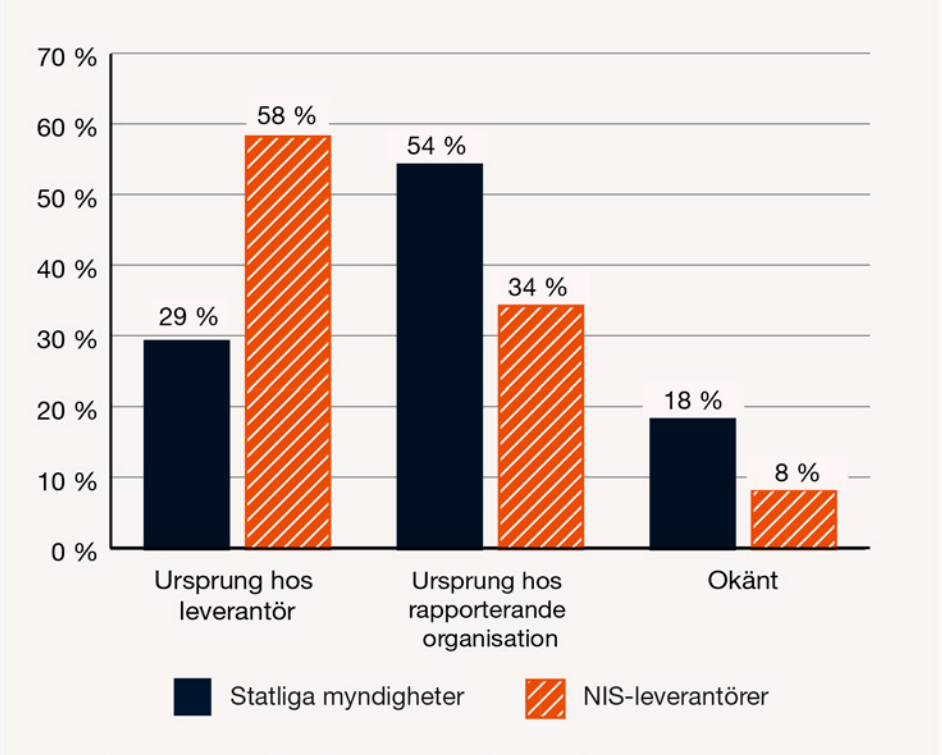
Myndigheten för civilt försvar ser allvarligt på förekomsten av detta mörkertal. Det underminerar myndighetens förmåga att ge en heltäckande nulägesbild samt analysera utvecklingen över tid. Det påverkar även myndighetens förmåga att ta fram ändamålsenligt och sektorsanpassat stöd till samhällsviktiga verksamhetsutövare. Myndigheten bedömer att en ökad efterlevnad av rapporteringsplikten är en grundförutsättning för att motståndskraften i det civila försvaret ska kunna öka.

Minskning av inrapporterade leverantörsincidenter

Under 2025 beskrev drygt 44 procent av inkomna cyberincidentrapporter att incidenten uppstått hos en leverantör. Det är en minskning i jämförelse med 2024, då 51 procent rapporterades ha uppstått hos en leverantör. Minskningen har varit störst bland statliga myndigheter. Skillnaden mellan åren ska förstås i sammanhanget av att det förekom två omfattade leverantörsincidenter både 2024 och 2025. Det handlar om cyberangreppet mot leverantören Tietoevry 2024, samt angreppet mot Miljödata 2025. Trots att de två leverantörsincidenterna var likartade, ledde den första till ett större antal incidentrapporter. Anledningen är delvis de skilda kraven på incidenter i beredskapsförordningen och NIS-förordningen, vilket gjorde angreppet mot Tietoevry till en rapporteringspliktig incident för fler organisationer.[10]

Diagram 4 redogör för att drygt 29 procent av inkomna cyberincidentrapporter från statliga myndigheter beskrev att incidenten skett hos en leverantör år 2025. Motsvarande siffra från 2024 var 48 procent. För NIS-leverantörer minskade andelen incidenter som hade sitt ursprung hos en leverantör från 62 procent år 2024 till 58 procent år 2025. Andelen med okänt ursprung har ökat i båda grupperna, men i synnerhet för incidentrapporter från statliga myndigheter, som ökade från fyra procent år 2024 till 18 procent år 2025.

Diagram 4. Andelen leverantörsincidenter 2025 för statliga myndigheter respektive NIS-leverantörer



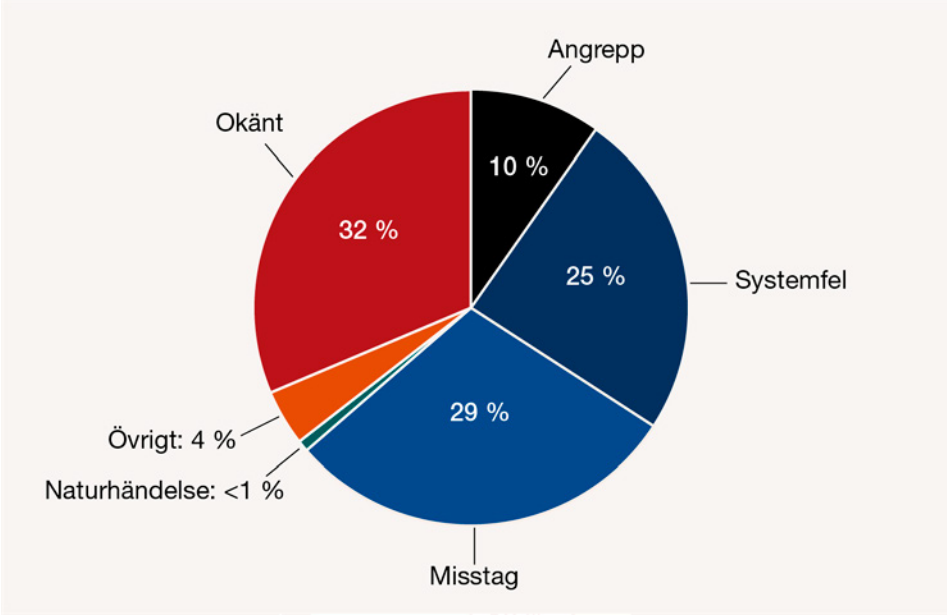
Not 10. Leverantörsincidenten hos Tietoevry blev rapporteringspliktig för många av Tietoevrys kunder som lyder under beredskapsförordningen. Incidenten hos Miljödata drabbade i högre utsträckning kommuner och regioner, som är rapporteringspliktiga enligt NIS-förordningen, än statliga myndigheter.

Misstag och systemfel fortsatt de vanligaste orsakerna

En cyberincident kan orsakas av flera olika typer av händelser. Myndigheten för civilt försvar delar övergripande in dessa händelser i kategorierna (i) misstag, (ii) angrepp, (iii) systemfel och (iv) naturhändelse.

Diagram 5 illustrerar fördelningen av orsaker bakom rapporterade cyberincidenter 2025. Under 2025 rapporterades majoriteten av incidenterna ha anledning ”okänd”, följt av misstag och systemfel. Av misstag och systemfel har den största andelen av cyberincidenterna uppstått till följd av genomförda ändringar inom it-miljön. Med undantag från 2023 har systemfel och misstag tidigare år uppgetts vara de vanligaste orsakerna bakom rapporteringspliktiga cyberincidenter, medan andelen incidenter med okänd anledning har ökat de senaste åren.

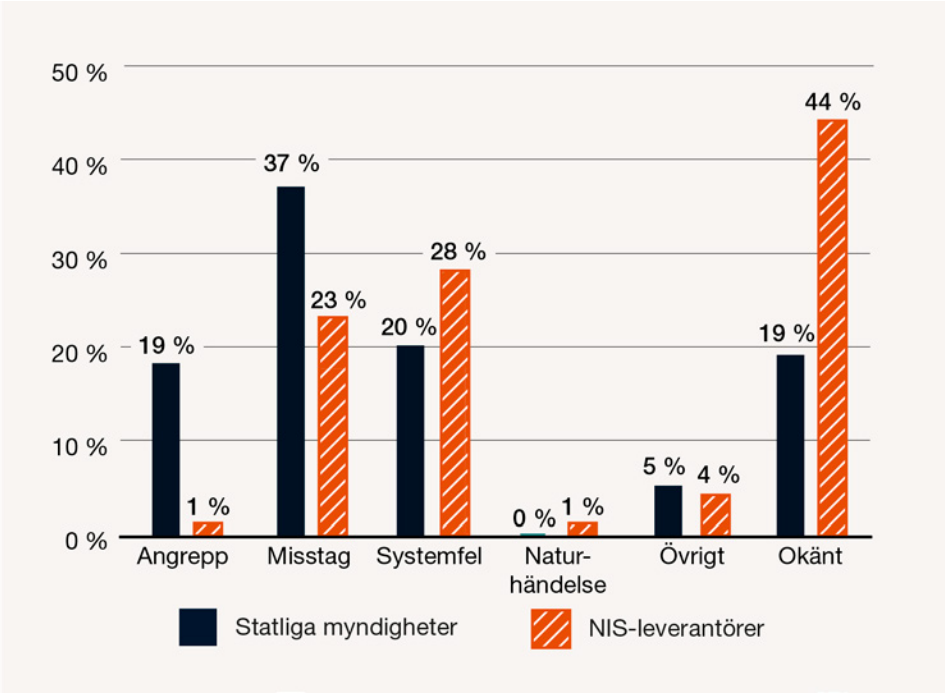
Diagram 5. Fördelning av rapporterade orsaker i incidentrapporteringen 2025



Fördelat på statliga myndigheter och NIS-leverantörer visar **diagram 6** att misstag är den mest frekvent rapporterade orsaken för statliga myndigheter under 2025, vilket skiljer sig från 2023 och 2024 då angrepp var den mest frekvent rapporterade orsaken. Liksom tidigare år har NIS-leverantörer rapporterat ytterst få angrepp. Det kan bero på att rapporteringsplikten ser olika ut vid cyberangreppsförsök mot NIS-leverantörer och statliga myndigheter.

Eftersom andelen incidentrapporter från NIS-leverantörer har ökat, kan detta ha bidragit till att andelen angrepp totalt har minskat, från 104 angrepp 2024 till 25 angrepp 2025. NIS-leverantörer ska rapportera cyberincidenter som har resulterat i en störning som är rapporteringspliktig. Myndigheten för civilt försvars bedömning är att det finns ett mörkertal avseende cyberincidenter orsakade av angrepp mot NIS-leverantörer.

Diagram 6. Rapporterade orsaker 2025 hos statliga myndigheter och NIS-leverantörer

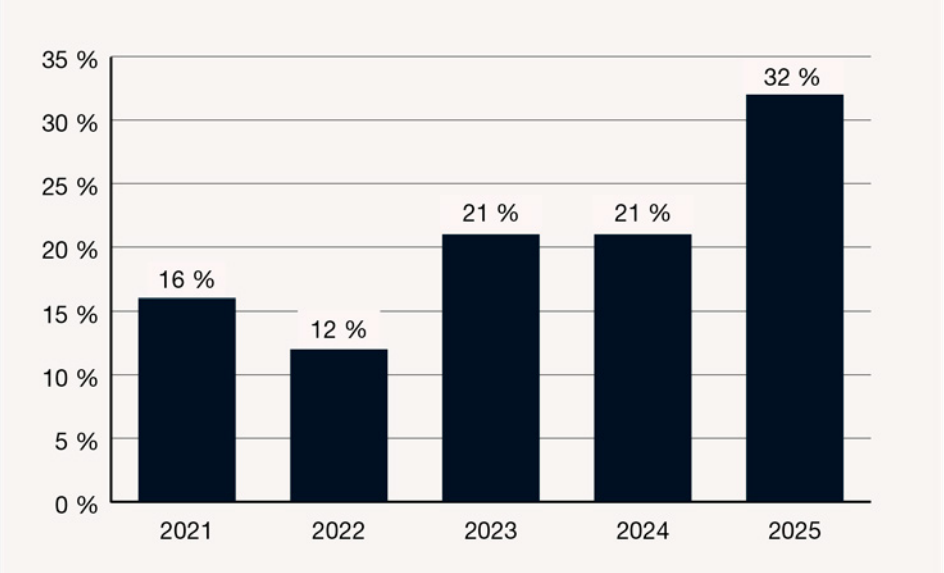


32 procent av inrapporterade orsaker uppgavs vara okända vid rapporteringstillfället under 2025. Liksom tidigare år står NIS-leverantörer för huvudparten av dessa rapporter. Däremot visar Myndigheten för civilt försvars analys att majoriteten av dessa incidenter inte är okända utan oftast kan härledas till systemfel, se avsnittet nedan.

Felrapportering från NIS-leverantörer bakom majoriteten av okända orsaker

Under 2025 uppstod majoriteten av incidenterna av okänd anledning, och utgör en ökning i jämförelse med tidigare år, se **diagram** 7.

Diagram 7. Fördelning av incidentrapporter med okänd orsak 2021–2025



Myndigheten för civilt försvar kan inte med säkerhet avgöra vad ökningen beror på, men det kan delvis vara kopplat till att det företrädelsevis är NIS-leverantörer som uppger okänd anledning bakom incidenterna som inrapporteras. NIS-leverantörer står nämligen för en större andel av samtliga inrapporterade incidenter i takt med att statliga myndigheter har inkommit med allt färre rapporter för varje år. 2023 stod NIS-leverantörer för nästan 74 procent av incidentrapporterna med okänd orsak, nästan 79 procent år 2024, och nästan 72 procent år 2025.

Myndigheten för civilt försvar har även kartlagt bakgrunden till incidenterna med okänd orsak genom fritextsvaren i incidentrapporterna, och kommit fram till att majoriteten av dessa kan härledas till systemfel.

Ofta har de inrapporterade organisationerna beskrivit incidentens händelseförlopp i detalj, men saknat information om den utlösande orsaken till incidenten, och angett orsaken som okänd. Det kan till exempel handla om att en mjukvara inte startar korrekt efter en planerad säkerhetsuppdatering, där organisationen kan identifiera den felande programkoden i mjukvaran men inte fastställa orsaken och därmed rapporterar orsaken till incidenten som okänd. Det kan även handla om gedigna och utförliga utredningar av orsaken bakom incidenter, där organisationens analys pekar ut ett särskilt systemfel, men att organisationen inte fullt ut kunnat verifiera den exakta orsaken, och rapporterat den som okänd. Myndigheten för civilt försvar bedömer i exemplen ovan att orsakerna bakom incidenterna är kända för den inrapporterade organisationen.

Felrapportering kan bland annat bero på okunskap hos anmälaren eller otydligheter i Myndigheten för civilt försvars stöd eller verktyg för inrapportering. Myndighetens skriftliga stöd och verktyg har samtidigt inte förändrats under de senaste åren.

Andelen cyberangrepp i incidentrapporterna har minskat

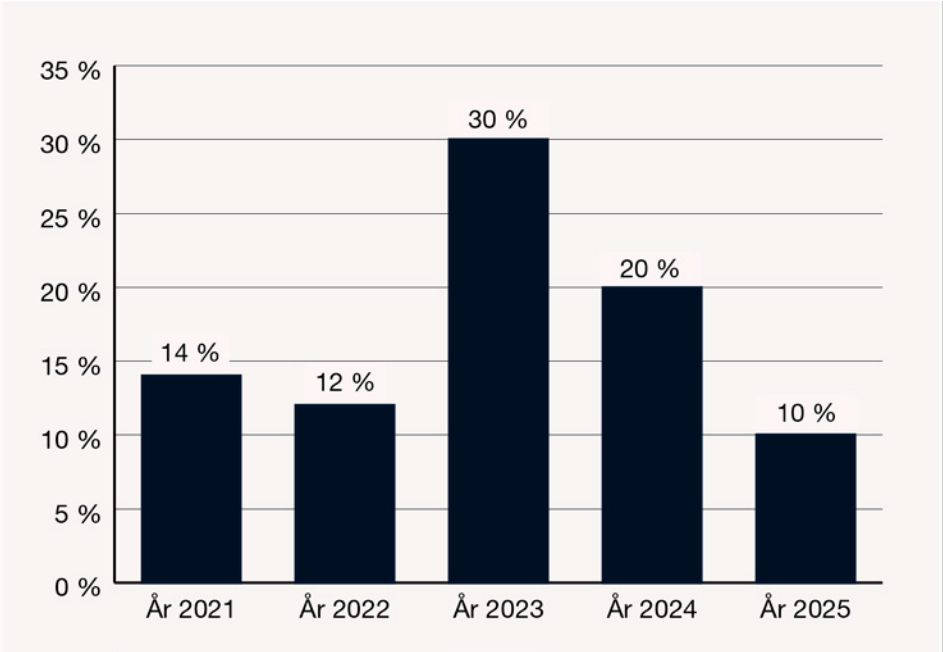
Andelen inrapporterade angrepp har minskat de senaste åren från 30 procent år 2023, till 20 procent 2024 och 9 procent år 2025. Sett till utvecklingen sedan 2021 visar **diagram 8** att inget år har haft en så låg andel inrapporterade angrepp som 2025. Den minskade andelen cyberangrepp kan ha flera förklaringar. Det beror delvis på att antalet cyberangrepp 2023 var ovanligt högt. Andra år har istället systemfel och misstag varit de vanligaste orsakerna till cyberincidenter. År 2023 utsattes verksamhetsutövare i Sverige för särskilt många överbelastningsangrepp under samma period som flera uppmärksammade manifestationer hölls där koranen brändes.

År 2024 utgjorde angreppet mot Tietoevry och dess följdincidenter en betydande andel av cyberangrepp i incidentrapporterna, medan cyberangreppet mot Miljödata 2025 inte genererade lika många incidentrapporter. Skillnaden beror till viss del på att angreppet mot Tietoevry blev rapporteringspliktigt för fler organisationer än angreppet mot Miljödata. Läs mer i avsnittet, Minskning av inrapporterade leverantörsincidenter. Myndigheten för civilt försvar kan

däremot inte bedöma i vilken utsträckning utvecklingen beror på ett faktiskt minskat antal cyberangrepp mot rapporteringspliktiga verksamhetsutövare, eller minskad rapporteringsvilja hos verksamhetsutövare.

Cyberangrepp får ofta stor uppmärksamhet trots att konsekvenserna kan vara lika allvarliga när kritiska system slås ut av misstag eller systemfel. Eftersom de inrapporterade angreppen utgör en liten del av alla incidenter är det nödvändigt för verksamhetsutövare att tillämpa ett allriskperspektiv i sina analyser för att upprätthålla samhällsviktiga verksamheters tjänster.

Diagram 8. Fördelning av rapporterade angrepp sedan 2021



Av cyberangrepp är överbelastningsangrepp den mest frekvent rapporterade angreppsmetoden 2025, precis som under 2023 och 2024. Totalt utgjorde överbelastningsangrepp drygt fyra procent av de inkomna incidentrapporterna år 2025. Även om överbelastningsangrepp endast stod för en liten del av de inkomna incidentrapporterna år 2025 kan angreppen likväl uppfattas som destruktiva. Angreppen kan få stor medial uppmärksamhet och påverka många personer i vardagen, men Myndigheten för civilt försvar bedömer att överbelastningsangrepp sällan får stor eller långvarig påverkan.

Överbelastningsangrepp mot Sveriges Television

Under juni 2025 utsattes Sveriges Television (SVT) för tre omfattande överbelastningsangrepp som påverkade delar av deras digitala utbud. SVT uppgav att det var oklart vem som låg bakom angreppen och om angreppen hade ett samband med varandra, men att trafiken kom från flera olika länder. Trots att angreppen inte innebar några stora konsekvenser beskrev SVT ett av angreppen som det största mot SVT hittills och betonade den digitala sårbarheten i dagens samhälle. Enligt Polisen var angreppen en del av en påverkanskampanj och syftade inte till att förstöra eller komma åt känsliga data.[11] Myndigheten för civilt försvar bedömer att överbelastningsangreppen resulterade i att ”nytta förhindrades” i och med att SVT inte kunde nå ut med vissa tjänster. Utifrån myndighetens analysramverk bedöms angreppet ha haft måttlig samhällspåverkan eftersom endast enstaka delar av SVT:s utbud påverkades. Samhällspåverkan uppstår, enligt Myndigheten för civilt försvars analysmetodik, när händelser medför konsekvenser för samhällsviktiga funktioner, tjänster eller grundläggande värden. Idag är SVT en samhällsviktig verksamhet i enlighet med cybersäkerhetslagen och som konsekvens ger störningar hos SVT påverkan på samhällsnivå.

Samtidigt är detta ett exempel på att vissa överbelastningsangrepp har blivit mer intensiva och svårhanterliga, samt att det blivit svårare att identifiera aktören bakom angreppen.

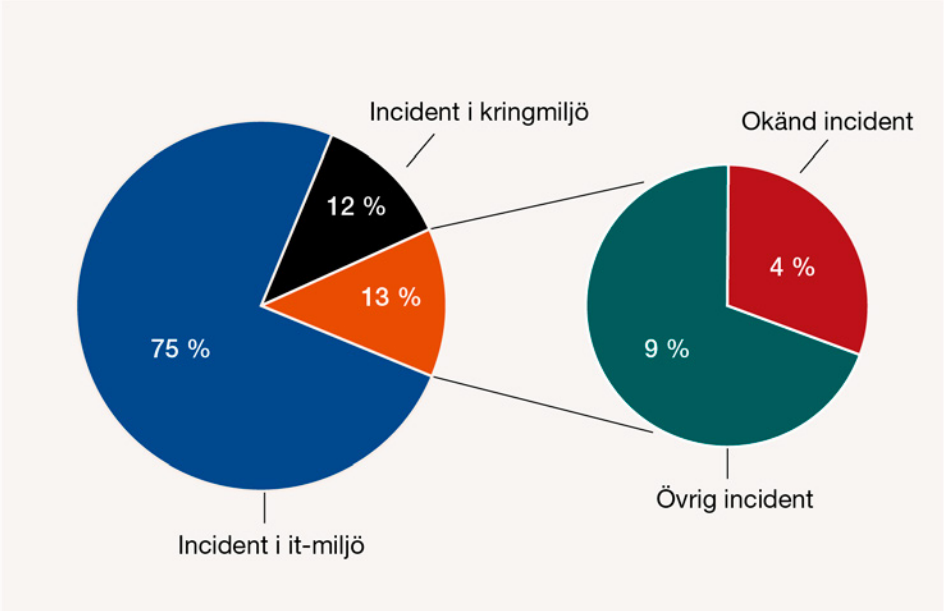
Cyberincidenter uppstår ofta i it-miljön

Liksom tidigare år uppger de flesta rapportörer att cyberincidenten uppstått inom it-miljön, det vill säga i ett eller flera informationssystem, snarare än kringmiljön. Fördelningen illustreras i **diagram 9**.

Med kringmiljön menas här den infrastruktur som är nödvändig för att upprätthålla ett eller flera informationssystem, inkluderande värme- och kylsystem, energiförsörjning eller fysiska förbindelser med komponenter. Cyberincidenter i kringmiljön orsakas ofta av att en förbindelse upphört. En större andel av dessa incidenter har uppstått som konsekvens av strömavbrott.

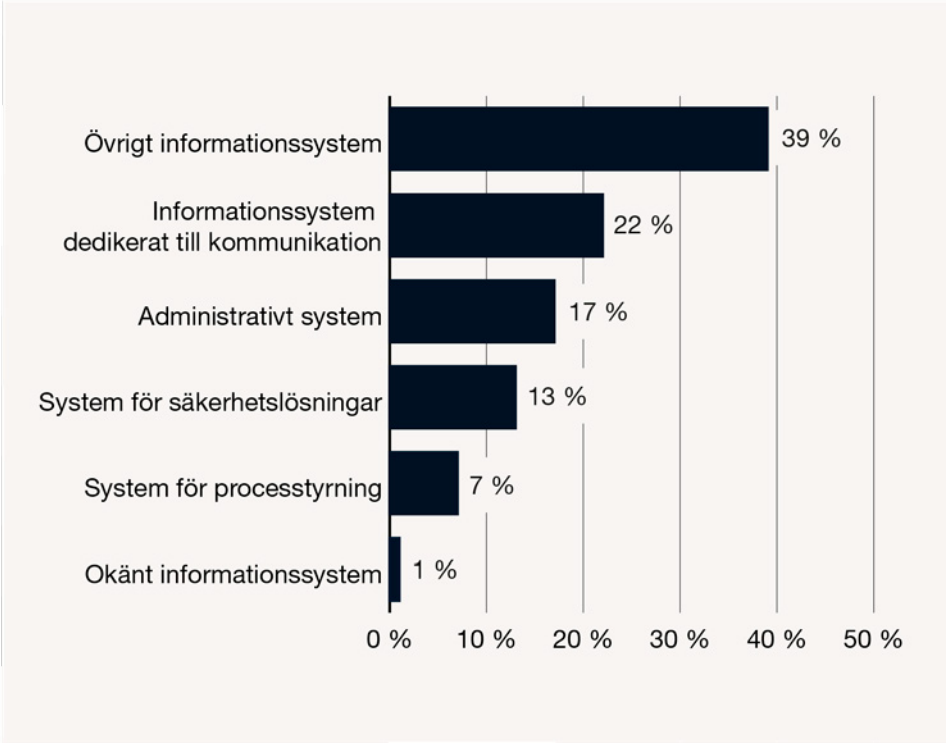
Not 11. Sveriges Television, ”Överbelastningsattacker mot SVT utreds med MSB – Den största SVT drabbats av”, [Sveriges Television], hämtad 2025-12-08; Sveriges Television, ”SVT utsatt för en ny överbelastningsattack”, [Sveriges Television], hämtad 2025-12-08.

Diagram 9. Cyberincidentens rapporterade ursprung



Av **diagram 10** framgår att bland de cyberincidenter som har sitt ursprung i it-miljön har de allra flesta uppgett att cyberincidenten uppstått i ”övrigt informationssystem”, alltså informationssystem som inte specificeras närmare i respektive incidentrapporteringsformulär. Det handlar ofta om journalsystem, trygghetslarm och säkerhetslösningar.

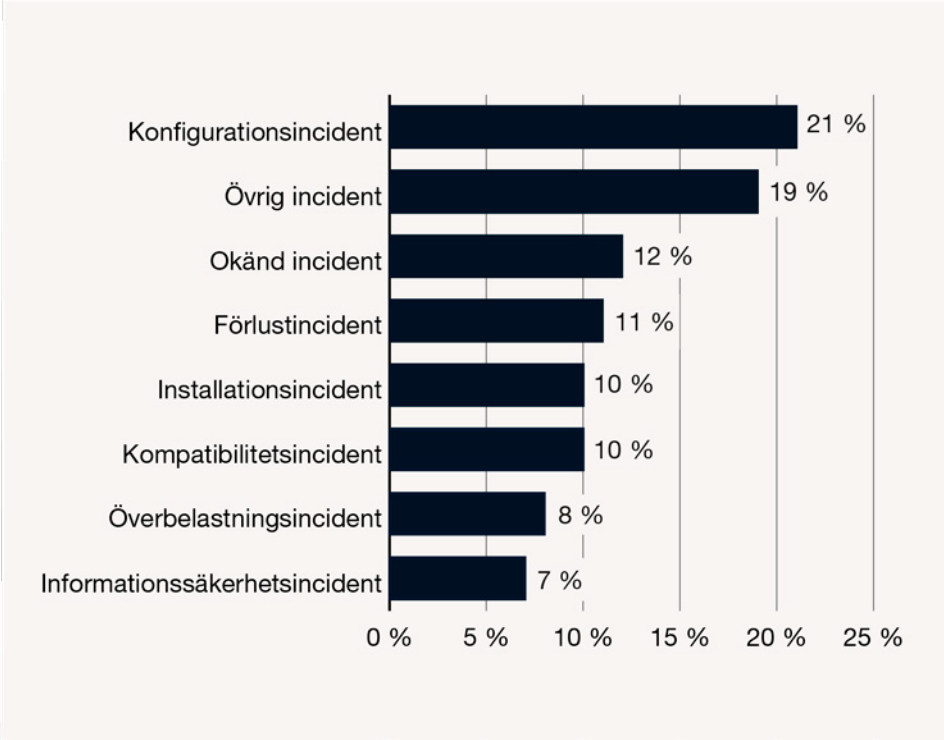
Diagram 10. Påverkad del av it-miljön 2025



Brister i rutiner för ändringshantering påverkar cybersäkerheten

Som tidigare nämnts är det vanligt förekommande att incidenter inträffar i samband med en genomförd ändring. I **diagram 11** åskådliggörs att den vanligaste typen av incident är en ”konfigurationsincident”, följt av ”övrig” och ”okänd” incident.

Diagram 11. Typer av cyberincidenter i it-miljön 2025



Myndigheten för civilt försvar har tidigare noterat att en stor andel av de cyberincidentrapporter som inkommer till myndigheten varje år, och som beskriver systemfel eller misstag som den bakomliggande orsaken, inträffat i samband med en ändring eller till följd av en utebliven ändring. Detta kan bero på att många rapporteringspliktiga organisationer saknar välfungerande rutiner för att genomföra ändringar i verksamhetskritiska informationssystem och nätverkskomponenter.[12]

För majoriteten av de som har uppgett svarsalternativ övrigt har typen av incident inte gått att fastställa. Utav dessa incidenter har drygt 94 procent påverkat någon aspekt av it-miljöns tillgänglighet. Det handlar till exempel om journalsystem, trygghetslarm eller säkerhetslösningar som inte uppnått fullgod tillgänglighet.

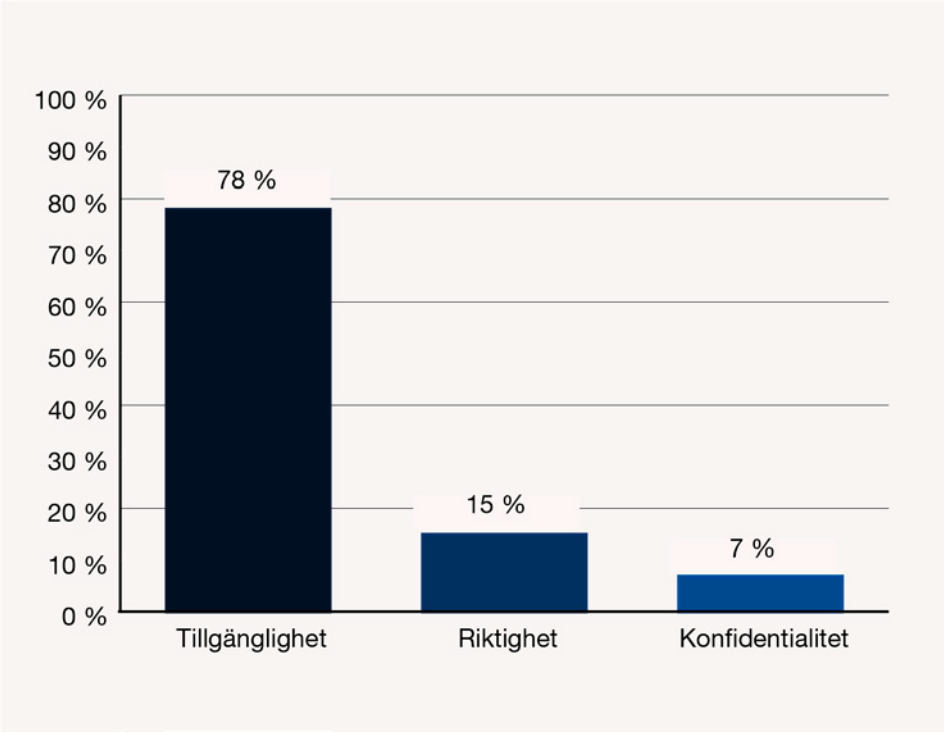
Not 12. Myndigheten för samhällsskydd och beredskap, *Ändringar som både hotar och skyddar – 20 rekommendationer för säkrare ändringar i våra informationssystem*, 2022.

Cyberincidenterna påverkar ofta informationssystemens tillgänglighet

Likt tidigare år visar **diagram 12** att majoriteten, 84 procent, av inkomna cyberincidentrapporter haft en påverkan på tillgängligheten till hela eller delar av ett eller flera informationssystem. Det är förvisso en minskning från 2024 då 90 procent angav påverkan på tillgänglighet, men likväl en ansenlig majoritet. Sammantaget innebär detta att rapporteringspliktiga cyberincidenter oftast uppstår som en konsekvens av att informationssystem och/eller informationstillgångar blir otillgängliga för användare.[13]

När cyberincidenter i 2025 års data påverkat riktigheten eller konfidentialiteten hos en informationstillgång har de oftast påverkat ett övrigt informationssystem eller ett ”administrativt system”. Drygt hälften av dessa incidenter består av handhavandefel, det vill säga misstag, och nästan en tredjedel av misstag som skett hos en leverantör.

Diagram 12. Andelen rapporterade cyberincidenter som har gett påverkan på tillgänglighet, riktighet och/eller konfidentialitet hos informationstillgångar av totalt antal incidenter, 2025



Anmärkning: incidenter kan påverka både tillgänglighet, riktighet och konfidentialitet samtidigt, därför uppgår staplarna tillsammans till mer än 100 %.

Not 13. En del av förklaringen till detta kan vara att rapporteringskrav i enlighet med NIS-lagstiftningen lägger stor vikt vid att förekomsten av, eller en betydande risk för, en störning i leveransen av en samhällsviktig tjänst.

En av de mest omskrivna cyberincidenterna som förekom under året är det cyberangrepp som drabbade systemleverantören Miljödata i augusti 2025. Trots att konsekvenserna av cyberincidenten drabbade en stor mängd kommuner och regioner, samtidigt som personuppgifter till över 1,5 miljoner privatpersoner publicerades på Darknet,[14] medförde angreppet inga störningar i tillgången till samhällsviktiga tjänster enligt Myndigheten för civilt försvars bedömning. Cyberincidenten hos Miljödata illustrerar däremot tydligt sårbarheten som uppstår när ett stort antal samhällsviktiga verksamheter, i detta fall kommuner och regioner, är beroende av samma digitala infrastruktur.

Noterbara incidenter från 2025 och dess påverkan

Nedan kan du läsa mer om hur myndigheten för civilt försvar bedömer påverkan på olika nivåer, utifrån svenska och utländska exempel på incidenter under 2025.

Analysen i denna rapport utgår från Myndigheten för civilt försvars analysmetodik för cybersäkerhet

Myndigheten för civilt försvar har tagit fram en analysmetodik för att analysera cybersäkerhet. Bland annat möjliggör metodiken att analysera enskilda cyberincidenters påverkan på verksamhetsutövarens it-miljö, verksamhet, eller, mer ovanligt, påverkan på samhället i stort.[15]

Påverkan på samhällsnivå handlar om påverkan på organisationers tjänster som möjliggör samhällets funktionalitet. Exempelvis vård, energi, betalningar eller transport, inom ett geografiskt område. På denna nivå bedöms hur en incident påverkar samhällets möjligheter att tillhandahålla grundläggande tjänster till medborgare, företag och andra aktörer.[16]

Myndigheten kommer att publicera analysmetodiken som ett samlat underlag under andra kvartalet 2026.

Utpressningsangreppet mot Miljödata, exempel på påverkan på flera nivåer

Den 23 augusti 2025 upptäcktes ett cyberangrepp mot systemleverantören miljödata. Miljödata levererar it-system till ett stort antal kunder i Sverige, inklusive Majoriteten av Sveriges kommuner. Angreppet var ett utpressningsangrepp där hotaktören genomförde dataintrång och hotade att lägga upp exfiltrerade upp-

Not 14. SVT, ”Experten: En miljon svenskars personuppgifter publicerade på darknet”, [Sveriges Television], hämtad 2026-03-03; Åklagarmyndigheten, ”Lägesuppdatering i ärende om bl.a. grovt dataintrång”, hämtad 2026-03-03.

Not 15. Se Myndigheten för civilt försvars analysmetodik bland annat i Myndigheten för samhällsskydd och beredskap, *It-incidenters påverkan, Ramverk för bedömning av påverkan på it-miljö, verksamhet och samhälle*, 2025.

Not 16. Myndigheten för civilt försvar bedömer bland annat att påverkan på samhällsnivå uppstår när samhällsviktiga och digitala tjänster påverkas. Till och med 2025 handlar det om statliga myndigheter under regeringen och verksamhetsutövare som är rapporteringspliktiga enligt NIS-förordningen. Från och med 2026 handlar det om organisationer som omfattas av cybersäkerhetslagen.

gifter på Darknet. När angreppet upptäcktes stängdes systemen ner och blev otillgängliga för Miljödatas kunder under olika långa perioder.[17]

När hotaktören senare publicerade de exfiltrerade uppgifterna bedömde Åklagarmyndigheten att 1,5 miljoner svenskars personuppgifter hade berörts.[18] I vissa fall hade även känsliga personuppgifter berörts, så som uppgifter till personer med skyddad identitet.[19] Personers vars personuppgifter har läckt kan bland annat utsättas för nätfiskeförsök.

Myndigheten för civilt försvars analysramverk gör det möjligt att jämföra incidenters påverkan på it-miljö, verksamhetsnivå och samhällsnivå utifrån ett antal kriterier.[20] Analyser av incidenters påverkan ska alltid avgränsas så att det blir tydligt vad analysen omfattar. Incidenten hos Miljödata ledde till exempel till att ”hot uppstod” i Miljödatas **it-miljö**, vilket i sin tur ledde till påverkan på Miljödatas **verksamhet**. För Miljödatas kunder ledde incidenten däremot till att ”framgångsfaktor upphörde”, då vissa system blev otillgängliga. Miljödatas kunder utgörs bland annat av samhällsviktiga verksamheter, och enstaka resurser hos kunderna, i form av system för olika ändamål, påverkades, men inte samhällsviktiga tjänster. Incidenten ledde därför inte till påverkan på samhällsnivå eftersom samhällspåverkan uppstår när händelser medför konsekvenser för samhällsviktiga funktioner, tjänster eller grundläggande värden. Myndigheten har inte kunnat göra en bedömning av omfattningen av påverkan på Miljödatas eller Miljödatas kunders verksamhet.

Utpressningsangreppet mot Jaguar, exempel på påverkan på verksamhetsnivå

Ett exempel på ett cyberangrepp som fick påverkan på verksamhetsnivå inträffade i Storbritannien under 2025. Det handlar om angreppet mot den brittiska biltillverkaren Jaguar. Angreppet riktades mot företagets it-miljö och ledde till att Jaguar tvingades stoppa produktionen i nära sex veckor, vilket beräknas ha kostat Storbritanniens ekonomi över 1,9 miljarder brittiska pund.[21] Störningen påverkade inte bara Jaguar, utan hela produktionskedjan. Omkring 5 000 företag, inklusive leverantörer, logistikföretag och tjänsteleverantörer som är beroende av Jaguars produktion, drabbades direkt av incidenten.[22]

Myndigheten för civilt försvar bedömer att utpressningsangreppet resulterade i att framgångsfaktor upphörde i och med att Jaguars verksamhet stängdes ner.

Not 17. SVT, ”Miljödata: Återställningen är snart klar”, [Sveriges Television], hämtad 2026-02-09.

Not 18. SVT, ”Experten: En miljon svenskars personuppgifter publicerade på darknet”, [Sveriges Television] hämtad 2026-02-09; Åklagarmyndigheten, ”Lägesuppdatering i ärende om bl.a. grovt dataintrång”, hämtad 2026-03-03.

Not 19. SVT, ”Sofias uppgifter läckta: ”Lever med skyddad identitet av en anledning”, [Sveriges Television] hämtad 2026-02-09.

Not 20. Se Myndigheten för civilt försvars analysmetodik bland annat i Myndigheten för samhällsskydd och beredskap, *Cyber-incidenters påverkan ”Ramverk för bedömning av påverkan på it-miljö, verksamhet och samhälle*, 2025.

Not 21. Computer Sweden, ”Cyberattacken mot Jaguar Land Rover slog mot Storbritanniens BNP” hämtad 2025-12-02.

Not 22. Cyber Magazine, “How JLR’s Category 3 Cyber Attack Caused Production Shutdown” hämtad 2025-12-02.

Nivån av påverkan i den aktuella it-miljön bedöms ha varit ”kritisk”, eftersom alla resurser i jaguars produktionsmiljö bedöms ha varit otillgängliga under september och delar av oktober.[23] Angreppet fick även påverkan på verksamhetsnivå, eftersom det resulterade i ekonomisk förlust samt påverkade verksamhetens intressenter. Påverkan på verksamhetsnivån bedöms ha varit allvarlig. Trots att angreppet mot Jaguar påverkade hela leveranskedjan, inklusive tusentals företag, och Storbritanniens BNP,[24] bedöms angreppet inte ha haft samhällspåverkan eftersom samhällspåverkan uppstår när händelser medför konsekvenser för samhällsviktiga funktioner, tjänster eller grundläggande värden.

Elavbrottet på Iberiska halvön, exempel på påverkan på samhällsnivå

Den 28 april 2025 drabbades Spanien och Portugal av ett intensivt elavbrott. Hela elnätet på den iberiska halvön, samt avgränsat område i Frankrike nära gränsen till Spanien omfattades.[25]

Elavbrottet utgjorde en händelse som ledde till många olika incidenter på Iberiska halvön. Elektroniska betalsystem, telekom och internettjänster upphörde delvis att fungera, bensinpumpar stannade och många upplevde att de inte nåddes av information från myndigheterna. Sjukhus och flygplatser förlitade sig på reservkraft.[26]

Elektriciteten återkom gradvis till olika regioner i Spanien och Portugal under kvällen, men totalt pågick händelsen i nästan 23 timmar.[27] En utredning inleddes av Spaniens förening för elnätsbolag som kom fram till att incidenten inträffade på grund av överspänning, det vill säga att den elektriska spänningen i elnätet var för hög, som spreds i en kedjeeffekt inom elnätet.[28]

Det är oklart exakt vad som orsakade den första överspänningen den 28 april och grundorsaken till händelsen är därmed okänd. Överspänning kan uppstå av flera olika anledningar, bland annat av blixtnedslag.

Händelsen hade påverkan på olika nivåer beroende på i vilka miljöer som händelsen ledde till incidenter. Till exempel uppstod incidenter i betalsystem och telenät, vilket Myndigheten för civilt försvar bedömer innebar allvarlig samhällspåverkan av typen ”framgångsfaktor upphör” eftersom det framstår som att mer än hälften av betalningssystemen respektive telenäten var ur tjänst.

Not 23. BBC, ”Jaguar Land Rover posts heavy loss after cyber-attack”, hämtad 2025-11-14.
Not 24. Ibid.;Computer Sweden, ”Cyberattacken mot Jaguar Land Rover slog mot Storbritanniens BNP” hämtad 2025-12-02.
Not 25. Entso-e, *Grid Incident in Spain and Portugal on 28 April 2025 ICS Investigation Expert Panel Factual Report*, 2025.
Not 26. BBC, “Everything went off: How Spain and Portugal’s massive power cut unfolded”, hämtad 2026-01-13.
Not 27. BBC, “How Spain powered back to life from unprecedented national blackout”, hämtad 2026-01-13.
Not 28. Energimarknaden, ”Överspänning orsakade spansk blackout”, hämtad 2026-01-13; The European Network of Transmission System Operators for Electricity, Grid Incident in Spain and Portugal on 28 April 2025, 2025; BBC, “Blackout in Spain and Portugal first of its kind, report finds”, hämtad 2026-01-13.

Tema

Cyberangreppens utveckling under 2023–2025

Tema: Cyberangreppens utveckling under 2023–2025

Hotaktörer omformar ständigt förutsättningarna för god cyberhygien. För att kunna förebygga och hantera dessa hot krävs en aktuell och samlad bild av hotet från cyberangrepp. I detta temakapitel har Myndigheten för civilt försvar analyserat utvecklingen av cyberangrepp under perioden 2023 till och med 2025 inom ett antal olika områden.

Detta temakapitel redogör för trender inom cyberangrepp inom ett urval av områden för perioden 2023 till och med 2025: antal cyberangrepp, utvecklingen av överbelastningsangrepp, användning av AI inom cyberangrepp, cyberangrepp mot leveranskedjor, cyberangrepp mot ot-system och utvecklingen av cyberangrepp inom cyberkrigföring i ljuset av kriget i Ukraina. Valet av områden har skett utifrån en bedömning baserat på Myndigheten för civilt försvars samlade bevakning inom cybersäkerhet. Därtill har analysen särskilt beaktat de områden som ingår i myndighetens samlingsbegrepp för cybersäkerhet: it-säkerhet, informationssäkerhet, ot-säkerhet och leveranskedjesäkerhet. Urvalet är inte heltäckande för utvecklingen inom cyberangrepp, och det kan finnas andra relevanta områden som ej förekommer i detta temakapitel.

Analysen i kapitlet bygger på information från dokumentstudier som bland annat inkluderar forskningsartiklar, myndighetsrapporter, samt information från nationella cybersäkerhetsorgan, så kallade CSIRT (Computer Security Incident Response Team)[29] och privata cybersäkerhetsföretag. Myndigheten för civilt försvar har gjort samlade bedömningar baserat på de analyserade källorna inom varje område, och kommenterat eventuella brister i tillgänglig information.

Kapitlet redovisar även statistik från Myndigheten för civilt försvars data över incidentrapporter, samt från en databas vid Center for International Security Studies vid universitetet i Maryland (CISSM). Mer information om detta återfinns i aktuella avsnitt. Alla underlag finns tillgängliga i publika källor med undantag från myndighetens egna data. Frågeställningen som har ställts till materialet har varit ”Hur har cyberangrepp utvecklats 2023–2025 inom de angivna områdena?”

Not 29. CSIRT står för ”Computer Security Incident Response Teams”. CSIRT-nätverket, som etablerades genom NIS-direktivet (EU) 2016/1148, är ett nätverk av nationellt utpekade CERT-funktioner för hantering av it-säkerhetsincidenter.

Analysen utgår från Myndigheten för civilt försvars analysmetodik för strategisk cybersäkerhet

Myndigheten för civilt försvar har tagit fram en analysmetodik för att analysera cybersäkerhet. Denna metodik tillämpas i analysen av cyberangrepp och innebär i korthet att cyberangrepp kan syfta till att orsaka skada hos den som angrips genom att förstöra viktiga informationstillgångar eller skapa oro. De kan också syfta till att förhindra nytta, exempelvis genom att störa samhällsviktiga tjänster. I vissa fall är målet att skapa nytta för angriparen, till exempel genom spionage, eller att förhindra skada för angriparen genom att störa försvarssystem eller kommunikation.[30]

Myndigheten kommer att publicera analysmetodiken som ett samlat underlag under 2026.

Oklart om totalt antal cyberangrepp globalt har ökat eller minskat

Det finns olika sätt att mäta utvecklingen av antalet cyberangrepp under perioden 2023–2025 och metoderna är inte helt jämförbara. Denna rapport redogör i tidigare kapitel för de cyberangrepp som framkommer i incidentrapporter till Myndigheten för civilt försvar. I incidentrapporterna framkommer en minskning av angrepp de senaste åren, från 30 procent år 2023, till 20 procent 2024 och 10 procent år 2025. Läs mer i avsnittet, Andelen cyberangrepp i incidentrapporterna har minskat.

Vissa rapporterar samtidigt om en ökning av antalet cyberangrepp i Ukraina och mot Ukrainas allierade från 2022 och framåt,[31] men med andra mätverktyg förekommer endast en ökning fram till 2024.[32] Myndigheter i Ukraina rapporterar till exempel om en stor ökning av cyberincidenter 2024–2025, men

Not 30. Se Myndigheten för samhällsskydd och beredskap, *När kriget kom nära – Årsrapport it-incidentrapportering 2022*, 2023, s. 50.

Not 31. National Cyber Security Centre of UK, *Annual review*, 2024, s.17; National Cyber Security Centre of UK, ”UK and allies expose Russian intelligence campaign targeting western logistics and technology organisations”, hämtad 2025-11-12; European Union Agency for Cyber Security, *Enisa Threat Landscape 2024*, 2024, s.11; European Union Agency for Cyber Security, *Enisa Threat Landscape 2023*, 2023, s.11; State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force, *War And Cyber: Three Years Of Struggle And Lessons For Global Security – Analytical Report*, Kyiv, 2025, s. 6.

Not 32. CISSM Cyber Events Database, “Cyber Events Database 2014-Dec 2025”, Centre for International and Security Studies at Maryland (CISSM), University of Maryland, 15 januari 2026.

i data från CISSM förekommer endast en mindre ökning under samma period.[33] Antalet cyberangrepp globalt tycks ligga på en mycket lägre nivå efter, jämfört med under, den fullskaliga invasionen av Ukrainas inledande fas.

Flera rapporterar om ökat antal angrepp mot Ukraina och Ukrainas allierade

Flera rapporterar om en ökning av antalet cyberangrepp mot västländer, Natoländer, och länder som stödjer Ukraina i kriget. Till exempel rapporterade Storbritanniens nationella cybersäkerhetscenter 2024 att Ryssland har intensifierat sina cyberoperationer[34] mot Ukraina och Ukrainas allierade för att stödja Rysslands militära kampanj.[35] Det är dock otydligt hur den brittiska myndigheten kom fram till denna slutsats.

Även EU:s byrå för nät- och informationssäkerhet (Enisa), har kommit fram till att antalet cyberangrepp ökade mellan andra halvan av 2022 till andra halvan av 2024,[36] framförallt mot medlemsstater i EU men även globalt. Enisas metod för att beräkna cyberangrepp är dock inte direkt jämförbar med Myndigheten för civilt försvars syn på cyberangrepp. Enisa samlar in data över cyberincidenter, gör en analys av vilket typ av ”hot” incidenten kan kopplas till, och presenterar statistik över antalet incidenter fördelat i olika hot. Hotkategorierna inkluderar bland annat överbelastningshot, hot mot leveranskedjor, hot från skadlig kod och hot från social manipulation.[37] Det är oklart hur kopplingen till olika hot görs. Därtill baserar Enisa sin data på cyberincidenter hämtade från öppna källor. Därmed är det inte säkert att antalet cyberangrepp faktiskt ökar, eller om den observerade ökningen är en följd av ökad uppmärksamhet om cyberangrepp som leder till att fler angrepp dokumenteras i öppna källor,[38] en brist som delas av databasen hos CISSM.

Ukrainas cybersäkerhetsmyndighet, State Service of Special Communications and Information Protection of Ukraine (SSSCIP) har rapporterat om en stor ökning av cyberincidenter till och med 2024, se **diagram 13**, och härleder ökningen till cyberangrepp från Ryssland. Samtidigt har antalet incidenter som har haft en ”kritisk

Not 33. State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force, *War And Cyber: Three Years Of Struggle And Lessons For Global Security – Analytical Report*, Kyiv, 2025, s. 6; CISSM Cyber Events Database, “Cyber Events Database 2014-Dec 2025” Centre for International and Security Studies at Maryland (CISSM), University of Maryland, 15 januari 2026.

Not 34. I myndigheten för civilt försvar innebär Cyberoperation en operation via cyberrymden i syfte att påverka en intern eller extern infrastruktur.

Not 35. CISSM Cyber Events Database, “*Cyber Events Database 2014–Dec 2025*” (Centre for International and Security Studies at Maryland (CISSM), University of Maryland, 15 januari 2026).

Not 36. Enisa presenterar sin data på ett annorlunda sätt för 2025 jämfört med tidigare år, vilket gör att en jämförelse över tid inte är möjlig.

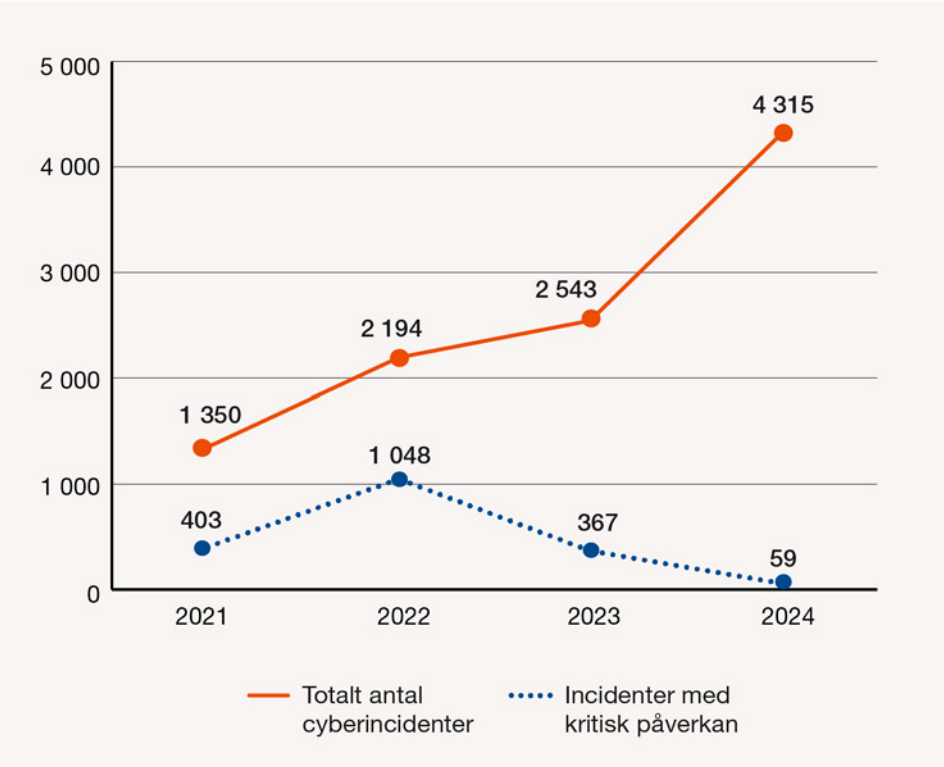
Not 37. European Union Agency for Cyber Security, *ENISA Threat Landscape 2022*, 2022, s. 88; European Union Agency for Cyber Security, *ENISA Threat Landscape 2023*, 2023, s. 4, 127; European Union Agency for Cyber Security, *ENISA Threat Landscape 2024*, 2024, s. 9–10; European Union Agency for Cyber Security, *ENISA Threat Landscape 2025*, 2025, s. 7–9.

Not 38. European Union Agency for Cyber Security, *Enisa Threat Landscape 2024*, 2024, s.11; European Union Agency for Cyber Security, *Enisa Threat Landscape 2023*, 2023, s.11.

påverkan på ukrainska organisationer”[39] sjunkit. SSSCIP anger att en anledning till detta är Ukrainas ökande förmåga att hantera allvarliga cyberangrepp.[40]

Information som tillgängliggörs i pågående konflikter ska dock antas vara publicerad under noggranna överväganden, och informationen kan vara ofullständig eller överdriven. Både Ryssland och Ukraina kan exponera motpartens motgångar men undvika att framhäva sina egna. Det är dessutom oklart hur ukrainska myndigheter definierar incidenter som har haft en kritisk påverkan, samtidigt som det är viktigt att skilja på incidenter som påverkar organisationer och incidenter som har samhällspåverkan.[41]

Diagram 13. Totalt antal cyberincidenter i Ukraina, varav antalet incidenter som lett till kritisk påverkan, åren 2021–2024



Källa: CERT-UA Registered Cyber Incidents, 2021–2024 (Quantity), i State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force, *War and Cyber: Three Years of Struggle and Lessons for Global Security – Analytical Report*, Kyiv, 2025, s. 6.

Not 39. Egen översättning av SSSCIP benämning ”Critical and high-level cyber incidents”. State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force, *War And Cyber: Three Years Of Struggle And Lessons For Global Security – Analytical Report*, Kyiv, 2025, s. 6.

Not 40. State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force, *War And Cyber: Three Years Of Struggle And Lessons For Global Security - Analytical Report*, Kyiv, 2025, s. 6.

Not 41. Läs mer om hur myndigheten för civilt försvar bedömer påverkan i Myndigheten för samhällsskydd och beredskap, *Cyber-incidenters påverkan – Ramverk för bedömning av påverkan på it-miljö, verksamhet och samhälle*, 2025.

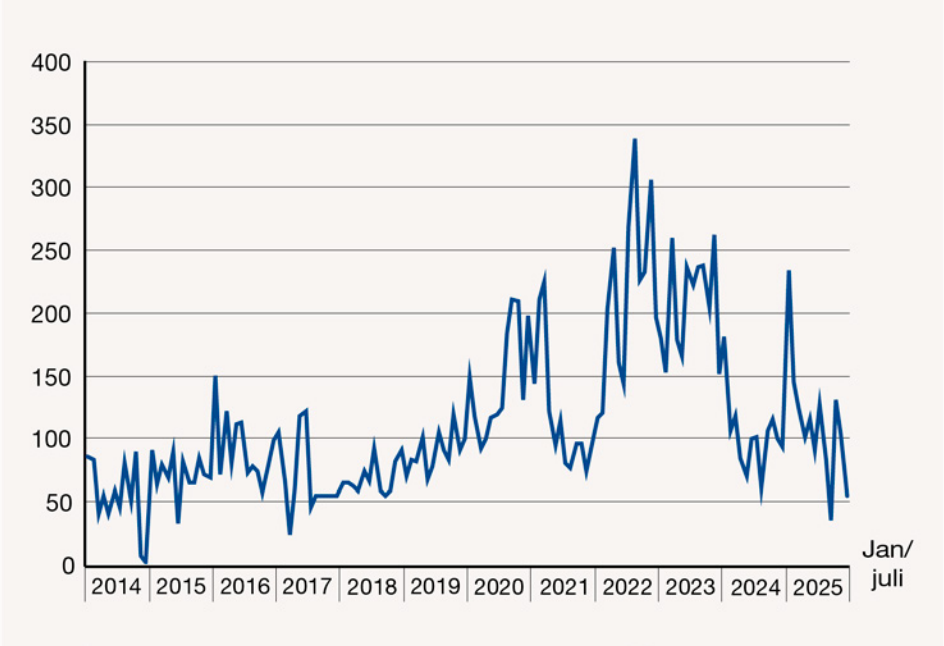
Antalet cyberincidenter i **diagram 13** kan tolkas som ett mått på antalet ärenden som har inkommit till Ukrainas nationella cybersäkerhetsorgan, CERT-UA, vilket inte nödvändigtvis innebär en ökning av antalet cyberangrepp utan ärenden kan även inbegripa andra incidenter så som handhavandefel. Det är även oklart om statistiken visar unika incidenter, eller om cyberangrepp mot till exempel en digital leveranskedja räknas flera gånger.

Metod som räknar cyberangrepp visar ett minskat antal sedan 2023

Antalet cyberangrepp globalt ökade avsevärt under 2022 och 2023.[42] Det är däremot oklart hur antalet cyberangrepp har utvecklats under åren därefter, 2024–2025. Som tidigare nämnt rapporterar flera aktörer om en ökning av cyberangrepp mot västländer, Nato-länder, och länder som stödjer Ukraina i kriget. Men det är ofta otydligt hur dessa slutsatser har dragits, och handlar ibland om antalet incidenter snarare än antalet cyberangrepp. Forskningsinstitutet Center for International Security Studies vid universitetet i Maryland (CISSM) har istället undersökt antalet cyberangrepp, i kontrast till antalet incidenter.

Enligt institutet har det skett en minskning av antalet cyberangrepp sedan krigets inledande fas. Det handlar om en återgång till ungefär samma nivåer som innan Rysslands fullskaliga invasion av Ukraina, se **diagram 14**.

Diagram 14. Antalet cyberangrepp globalt, åren 2014–2025, fördelat på månad



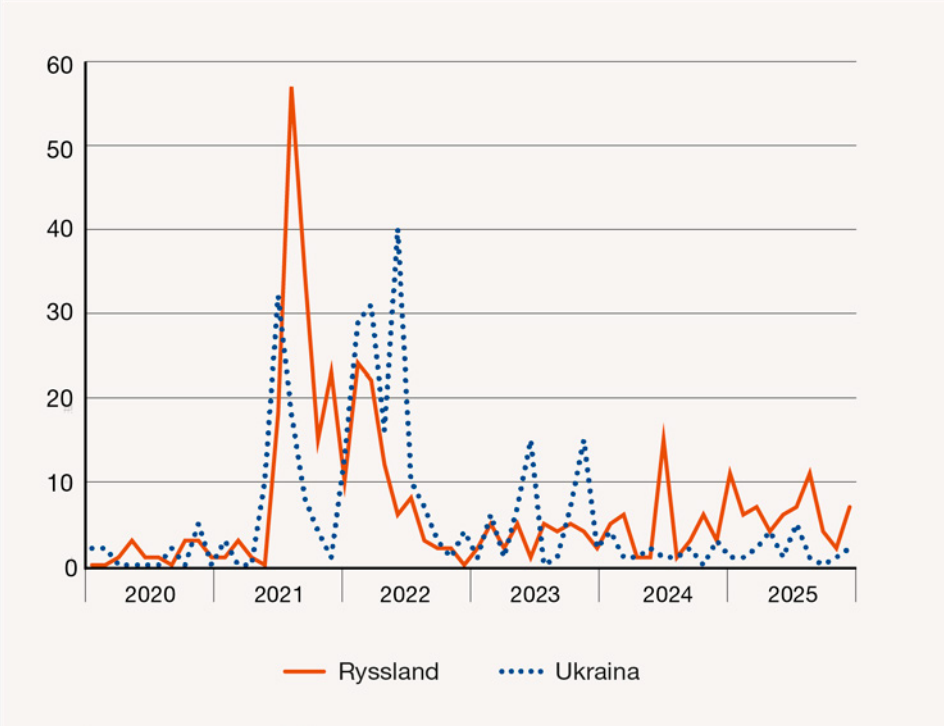
Källa: CISSM Cyber Events Database, “Cyber Events Database 2014-Dec 2025” (Centre for International and Security Studies at Maryland (CISSM), University of Maryland, 15 januari 2026).

Not 42. Se bland annat CISSM Cyber Events Database, “Cyber Events Database 2014-Dec 2025” Centre for International and Security Studies at Maryland (CISSM), University of Maryland, 15 januari 2026.

Metoden som forskningsinstitutet använder går ut på att webbskrapa nyhetsartiklar från internet, på drygt 60 olika språk, som innehåller nyckelord som kan kopplas till cyberangrepp. Därefter gör institutet en kvalitativ bedömning av innehållet i artikeln för att se till att ett angrepp inte räknas två gånger. De lägger till annan data, till exempel om vilken typ av hotaktör som har genomfört angreppet, om motivet bakom angreppet är finansiellt eller avser ett annat syfte, vilket land som är drabbat och i vilket land hotaktören befinner sig. Denna metod avser att endast räkna ett cyberangrepp en gång, oavsett hur många incidenter som uppstår.

Statistiken visar bland annat att cyberangrepp mot mål i Ryssland och Ukraina var mer frekventa under den fullskaliga invasionens inledande fas, men att antalet angrepp var långt färre efter, jämfört med under, 2022, se **diagram 15**.[43] Som nämnts tidigare skulle en anledning till detta kunna vara att rapporteringen om cyberangrepp i kriget avtog efter en tid.

Diagram 15. Antalet cyberangrepp mot mål i Ryssland respektive Ukraina åren 2020–2025, fördelat på månad



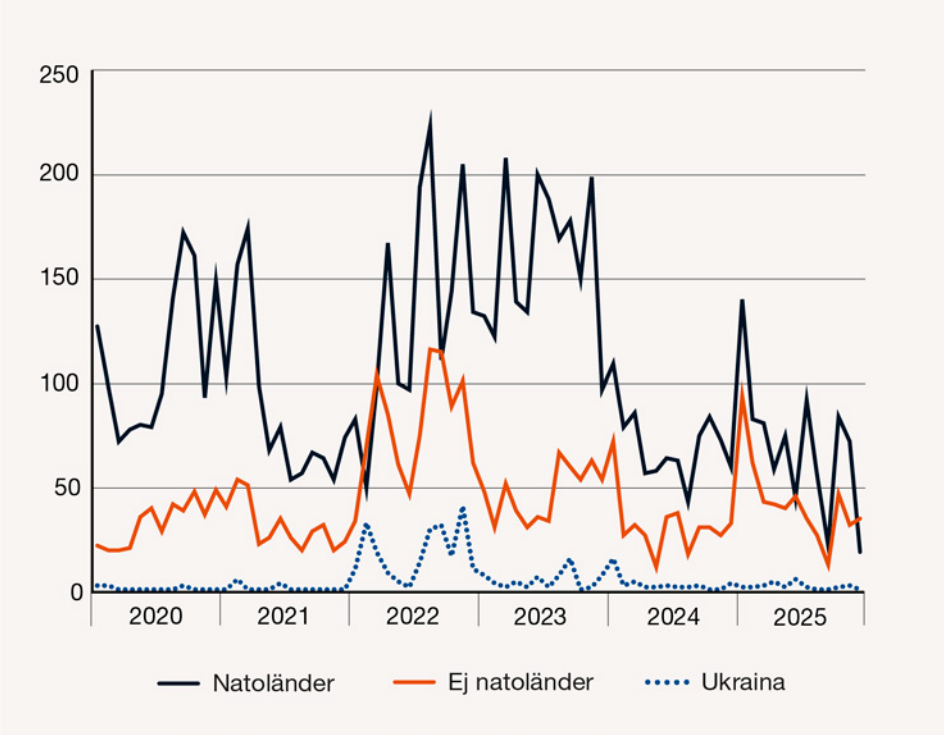
Källa: CISSM Cyber Events Database.

Not 43. Eftersom datan, liksom Enisas data, baseras på cyberincidenter hämtade från öppna källor är det inte säkert att antalet cyberangrepp stämmer överens med det faktiska antalet inträffade angrepp, eller om statistiken är en följd av uppmärksamhet om cyberangrepp som leder till att angrepp dokumenterades i öppna källor.

Det kan även nämnas att myndigheten för civilt försvar har utvecklat en egen metod för att bedöma om ett cyberangrepp når angriparens syfte, se Myndigheten för samhällsskydd och beredskap, *Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp*, 2024, s. 21–30.

Statistiken visar även att antalet angrepp mot Nato-länder var fortsatt höga även 2023, men därefter återgick antalet angrepp till en lägre nivå, se diagram 16.

Diagram 16. Antalet cyberangrepp mot Natoländer, icke-Natoländer och Ukraina, åren 2020–2025, fördelat per månad



Källa: CISSM Cyber Events Database.

En anledning till att vissa rapporterar om att cyberangrepp har ökat medan statistiken som presenteras i diagrammen ovan visar en minskning kan vara att olika metoder används för att framställa statistiken. Om till exempel angrepp i högre grad utförs mot leveranskedjor, kan det skapa fler incidentrapporter än antalet cyberangrepp. Ett enskilt angrepp mot en leverantör kan få följdverkningar hos ett stort antal organisationer i leveranskedjan. Läs mer om detta i avsnittet, Angrepp mot digitala leveranskedjor kan ha ökat i vissa avseenden.

AI har möjliggjort effektivisering av cyberangrepp

Artificiell intelligens (AI) har under de senaste åren framställts som ett kraftfullt verktyg för så väl cyberangrepp som i cyberförsvar. Flera aktörer rapporterar om att användningen av AI i cyberangrepp har ökat samt effektiviserat vissa typer av angrepp. Det handlar om utveckling av nätfiske och skadlig kod, automatisering av angrepp och identifiering av sårbarheter.[44]

Not 44. Se till exempel National Cyber Security Centre of UK, "The near-term impact of AI on the cyber threat" hämtad 2025-11-19; Google, *Cybersecurity Forecast 2026*, 2025, s. 4.

Det är dock viktigt att beakta att dessa rapporter i huvudsak kommer från privata företag som säljer olika cybersäkerhetstjänster, och från myndigheter vars källor bland annat utgörs av samma privata företag. Redogörelsen för vad litteraturen visar bör förstås mot denna bakgrund, och Myndigheten för civilt försvar har i sin analys beaktat detta.

Rapporterna vittnar samtidigt om en utveckling som stämmer överens med Myndigheten för civilt försvars tidigare analyser och utvecklingen av AI innebär självklara teknologiska möjligheter för hotaktörer, till exempel inom avancerat nätfiske och automatisering av angrepp. Sammantaget är det svårt att bedöma i vilken utsträckning användningen av AI har ökat inom angrepp och angreppsmetoder, men det finns en tydlig risk för att detta kommer att ske framgent.

Användningen av AI ökar och effektiviserar cyberangrepp enligt företag och vissa myndigheter

Många privata företag har rapporterat att användningen av AI i cyberangrepp har ökat under de senaste åren.[45] Särskilt nämnvärda analyser kommer från Microsoft, som rapporterar att det har blivit allt vanligare att använda AI i cyberangrepp mellan 2022 och 2025, där angreppens hastighet, omfattning och komplexitet har ökat i takt med utvecklingen och användningen av AI. Microsoft skriver att hotaktörer använder AI för att effektivisera automatiseringen av hela angreppskedjan, där så kallade AI-agenter kan generera och sprida skadlig kod, identifiera och utnyttja sårbarheter och anpassa sig i realtid för att kringgå säkerhetsspärrar. Detta kan göra det möjligt för hotaktörer att genomföra angrepp i stor skala, mot många mål samtidigt och med minimal resursåtgång.[46]

Flera aktörer har rapporterat att integrationen av generativ AI har ökat precisionen och omfattningen i cyberangrepp, utpressningsangrepp och social manipulation,[47] där Enisa rapporterade 2025 att AI-genererade nätfiskekampanjer stod för mer än 80 procent av alla angrepp med social manipulation världen över.[48]

Även vissa myndigheter och statligt kopplade organisationer har rapporterat om en ökning av användning av AI i cyberangrepp hos statliga aktörer. Enligt

Not 45. Se till exempel Microsoft, *Microsoft Digital Defense Report 2025*, 2025, s. 49; DeepStrike, ”AI Cyber Attacks Statistics 2025, Trends, Costs, Defense”, hämtad 2026-02-11; Check Point Software Technologies, *Cyber Security Report 2026*, 2026, s. 50; Evertrust Consulting, “AI-användning vid cyberattacker ökar kraftigt”, hämtad 2026-02-11.

Not 46. Microsoft, “Staying ahead of threat actors in the age of AI”, hämtad 2025-11-25; Microsoft, *Microsoft Digital Defense Report 2025*, 2025.

Not 47. The European Union Agency for Cybersecurity, *Enisa Threat Landscape 2023*, 2023, s. 4, 74; Gartner, “Gartner Survey Reveals GenAI Attacks Are on the Rise”, hämtad 2026-02-11; Check Point Software Technologies, Cyber Security Report 2026, 2026, s. 17, 55; Research Institutes of Sweden, ”AI förändrar cybersäkerheten och hotbilden”, hämtad 2026-02-11; Microsoft, *Microsoft Digital Defense Report 2025*, 2025, s. 14; Microsoft, “Extortion and ransomware drive over half of cyberattacks”, hämtad 2025-11-25.

Not 48. The European Union Agency for Cybersecurity, *Enisa Threat Landscape 2025*, 2025, s. 5.

Enisa har statligt kopplade hotaktörer i Ryssland, Kina, Iran och Nordkorea kraftigt ökat sin användning av AI för att utveckla sina cyber- och påverkansoperationer.[49] Att Ryssland har utökat sin användning av AI har även rapporterats av Regional Cyber Defence Centre (RCDC), en internationell cybersäkerhetsorganisation under Litauens nationella cybersäkerhetscenter.[50] RCDC menar att Ryssland i allt högre grad har integrerat AI i sina cyberoperationer från 2023 till 2025. Det handlar bland annat om att AI-genererad röstkloning har lett till att ryska aktörer som bedriver utpressningsangrepp och nätfiske har ökat sina telefonbedrägerier med 442 procent i slutet av 2024.[51] 2025 rapporterade även CERT-UA att det skett en ökning av ryska AI-genererade cyberangrepp mot Ukraina i form av nätfiske och skadlig kod.[52]

AI har skapat möjlighet för fler aktörer att utföra angrepp och utöva digitalt försvar

Enligt det brittiska nationella cybersäkerhetscentret har AI sänkt tröskeln för eventuella framtida cyberkriminella att kunna genomföra cyberangrepp. Detta innebär att personer eller grupper som tidigare saknade kunskap, resurser eller tekniska färdigheter nu kan genomföra sina angrepp med hjälp av AI. Det brittiska cybersäkerhetscentret bedömer att denna ökade åtkomst sannolikt förväntas driva på en global ökning av utpressningsangrepp.[53]

Myndigheten för civilt försvar har tidigare rapporterat att den effektiva automatiseringen med AI bland annat har gjort att fler aktörer har möjlighet att genomföra cyberangrepp och att angreppen kan ske snabbare samt mot fler mål.[54]

Myndigheten för civilt försvars tidigare analys har även visat att utvecklingen av AI skapar förutsättningar för både angrepp och digitalt försvar, där AI gör det lättare att förutse angrepp och att upptäcka hot under en kortare tid.[55] Exempel på det förekom redan 2024, då Google meddelade att deras AI-agent hade identifierat en nolldagarssårbarhet i en produktionskod och åtgärdat den samma dag.[56]

Not 49. The European Union Agency for Cybersecurity, *Enisa Threat Landscape 2024*, 2024, s. 25.

Not 50. Rapporten är inrättad av Litauen och USA och har tagits fram i samarbete med ukrainska experter och andra regionala partners.

Not 51. The Regional Cyber Defence Centre, *A Comparative Study of Russian Offensive Cyber Capabilities*, 2025, s. 25.

Not 52. State Service of Special Communications and Information Protection of Ukraine, *Russian Cyber Operations – Analytics for the H1 2025*, 2025, s. 5.

Not 53. National Cyber Security Centre of UK, "The near-term impact of AI on the cyber threat" hämtad 2025-11-19.

Not 54. Myndigheten för samhällsskydd och beredskap, *Artificiell intelligens för obemannade luftfartyg vid samhällsstörningar*, 2022, s. 18–19.

Not 55. Myndigheten för samhällsskydd och beredskap, *Artificiell intelligens för obemannade luftfartyg vid samhällsstörningar*, 2022, s. 19–20; Microsoft, *Microsoft Digital Defense Report 2025,* 2025, s. 4–6.

Not 56. Google, "From Naptime to Big Sleep: Using Large Language Models to Catch Vulnerabilities in Real-World Code", hämtad 2025-12-18.

Även den amerikanska myndigheten Cybersecurity and Infrastructure Security Agency (CISA) använder AI för att automatisera identifieringen av hot, nätverksavvikelser och risker i stora datamängder.[57] Likväl har Taiwans försvarsdepartement en AI-byrå som inför AI-produkter med fokus på cyberförsvar.[58]

Överbelastningsangrepp har blivit mer avancerade och ökat i flera avseenden

Överbelastningsangrepp har varit den mest frekvent rapporterade angreppsmetoden till Myndigheten för civilt försvar under 2023–2025.[59] En anledning till det kan vara att överbelastningsangrepp är förhållandevis enkla att genomföra i jämförelse med andra angrepp. År 2025 rapporterade även Enisa att överbelastningsangrepp inte bara stod för flest incidenter, utan även påverkade flest sektorer inom EU.[60] Därtill har antalet överbelastningsangrepp ökat i vissa avseenden. Det handlar om en ökning av överbelastningsangrepp med geopolitiska motiv, ökat antal angrepp mot statliga aktörer och mot kritisk infrastruktur, samt att överbelastningsangrepp generellt har blivit mer omfattande och mer komplexa.[61] För Sverige kan detta framåt bland annat innebära en risk för överbelastningsangrepp i samband med valet 2026.

Överbelastningsangrepp har ökat i flera avseenden

Sveriges CSIRT-enhet tog under perioden 2022–2025 emot flest ärenden gällande överbelastningsangrepp under 2023, följt av 2025.[62] Även Estlands CSIRT-enhet, CERT-EE har sett en generell ökning av överbelastningsangrepp sedan 2021,[63] och företaget Cloudflare, som bland annat erbjuder tjänster för att blockera överbelastningsangrepp, har sett en ökning under 2025. Under 2025 blockerade de nästan dubbelt så många överbelastningsangrepp som under 2023.[64]

Not 57. United States Department of Homeland Security, "Cybersecurity and Infrastructure Security Agency – AI Use Cases", hämtad 2025-12-18.

Not 58. Taiwan News, "Taiwan launches AI office to boost smart defence tech", hämtad 2026-02-05.

Not 59. Se kapitel Rapporterade cyberincidenter under 2025; Myndigheten för samhällsskydd och beredskap, *Verktyg för ökad motståndskraft och stärkt civilt försvar*, 2025, s. 9.

Not 60. European Union Agency for Cyber Security, *ENISA Threat Landscape 2025*, 2025, s. 7, 15.

Not 61. National Cyber Security Centre of Estonia (RIA), "DDoS attacks: more noise, less impact", hämtad 2025-12-02; Nationellt Cybersäkerhetscenter, *Överbelastningsangrepp mot kritisk infrastruktur i Norden och Baltikum hösten 2024*, 2025, s. 3; Cloudflare, "Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS Threat Report", hämtad 2025-12-11.

Not 62. CERT-SE tar emot ärenden kopplade till bland annat överbelastningsangrepp. Mellan 2022 – 2025 varierade antalet ärenden, där flest inkom under 2023 och 2025 och minst under 2022 och 2024. Ett ökat antal ärenden innebär inte nödvändigtvis ett ökat antal incidenter, då ärenden är kopplade till inflödet av information till CERT-SE.

Not 63. National Cyber Security Centre of Estonia, "DDoS attacks: more noise, less impact", hämtad 2025-12-02.

Not 64. Cloudflare, "Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS Threat Report", hämtad 2025-12-11.

Det har även förekommit en koppling mellan antalet överbelastningsangrepp och geopolitik under den studerade perioden. EU:s CSIRT, CERT-EU, menar att överbelastningsangrepp används som ett strategiskt verktyg i geopolitiska spänningar för att skapa förvirring, och att det förklarar det ökade antalet och intensiteten av överbelastningsangrepp mot statliga aktörer. CERT-EU menar även att överbelastningsangrepp mot statliga aktörer ofta vidtas som svar på olika typer av symboliska handlingar, såsom löften om stöd till Ukraina.[65] I november 2025 drabbades exempelvis danska kommuner och partier av överbelastningsangrepp inför deras kommun- och regionval. Enligt en dansk myndighet utför den ansvariga hotaktören, med koppling till Ryssland, regelbundet överbelastningsangrepp mot webbplatser i olika europeiska länder i samband med val.[66] Ett annat tydligt exempel som inte hör till den studerade tidsperioden är överbelastningsangreppen mot grönländska webbplatser under februari 2026. Enligt ett danskt mediehus har den hotaktör som tagit på sig ansvaret för angreppen uppgett att angreppen genomförts som hämnd för att Danmark donerat stridsflyg till Ukraina.[67]

I Sverige har överbelastningsangrepp korrelerat både med Sveriges inträde i Nato, Sveriges stöd till Ukraina och med koranbränningarna 2023. Under 2023 rapporterade statliga myndigheter in ett stort antal överbelastningsangrepp i samband med koranbränningarna i Sverige.[68] Överbelastningsangreppen ökade i antal även i Sverige med 466 procent efter landets inträde i Nato i mars 2024, något som också drabbade Finland under landets Natoanslutning 2023, enligt data från företaget Cloudflare.[69] Under 2024 utsattes även Trafikverket och Transportstyrelsen för överbelastningsangrepp, där hotaktören som tog på sig ansvaret för angreppet uppgav att motivet var Sveriges beslut om militärt stöd till Ukraina.[70]

Särskilt statliga aktörer och kritisk infrastruktur har drabbats av ökat antal överbelastningsangrepp under tidsperioden. Sveriges nationella cybersäkerhetscenter (NCSC) har rapporterat att överbelastningsangrepp har ökat mot kritisk infrastruktur i både Europa och Sverige. Under 2024 riktades 757 överbelastningsangrepp mot mål i den svenska IP-rymden, varav nästan en tredjedel drabbade kritisk infrastruktur.[71] Riksbanken har även rapporterat att flera svenska banker och operatörer av finansiell infrastruktur utsattes för allvarliga överbelastningsangrepp under 2024 och 2025, vilket ledde till att banktjänster blev otillgängliga via mobilapplikationer. Enligt Riksbanken har motiven bakom överbelastningsangreppen varit geopolitiska.[72]

Not 65. CERT-EU, “DDoS Overview and Response Guide”, 2024, hämtad 2025-12-02.
Not 66. Dagens Nyheter, ”Cyberattack mot danska partier dagen före valet”, hämtad 2026-01-13.
Not 67. SVT, ”Cyberattacker mot Grönland – rysk hackergupp tar på sig ansvaret”, [Sveriges Television], hämtad 2026-03-16.
Not 68. Myndigheten för samhällsskydd och beredskap, *Verktyg för ökad motståndskraft och stärkt civilt försvar*, 2025, s. 9.
Not 69. Cloudflare, “DDoS threat report for 2024”, 2025-12-02.
Not 70. Trafikverket, *Öppen antagonistisk hotbild mot transportsektorn*, 2025, s. 42.
Not 71. Nationellt Cybersäkerhetscenter, *Överbelastningsangrepp mot kritisk infrastruktur i Norden och Baltikum hösten 2024*, 2025, s. 4–5.
Not 72. Sveriges Riksbank, *Distributed denial-of-service attacks in the financial sector*, 2025, s. 3–4, 6–7.

Överbelastningsangrepp har blivit mer komplexa

Vissa överbelastningsangrepp har blivit mer omfattande och komplexa under tidsperioden. Det handlar bland annat om överbelastningsangrepp som är mer intensiva än tidigare, så som överbelastningsangrepp mot Riksbanken och mot SVT. Riksbanken skriver att överbelastningsangreppen mot finanssektorn har blivit mer sofistikerade och omfattande än tidigare, främst eftersom angreppen är riktade mot specifika mål och utformade för att maximera effekten av angreppet.[73]

Enisa rapporterade redan 2022 att överbelastningsangrepp hade blivit allt större och mer komplexa och att cyberkrigföring var den främsta orsaken bakom sådana angrepp, särskilt cyberkrigföringen mellan Ryssland och Ukraina.[74] Även CERT-EU har rapporterat att överbelastningsangreppens intensitet mot statliga aktörer har ökat sedan Rysslands fullskaliga invasion av Ukraina. De skriver att angreppens metoder har utvecklats och att angreppen har blivit allt större och kraftfullare för varje år.[75] Även företaget Cloudflare har rapporterat att överbelastningsangrepp har blivit allt mer omfattande under de senaste åren och att den utvecklingen förväntas fortsätta.[76]

Angrepp mot digitala leveranskedjor kan ha ökat i vissa avseenden

Det finns anledning att tro att cyberangrepp mot de digitala leveranskedjorna har ökat under de senaste åren. Flera cybersäkerhetsföretag har rapporterat om en ökning av angrepp mot leveranskedjor i flera avseenden under de senaste åren, särskilt från 2024 till 2025. Tillsammans med rapporter från europeiska myndigheter kan detta indikera att angreppen mot leveranskedjor har ökat. Slutsatser bör dock dras med försiktighet bland annat för att det saknas tillräckliga data inom området, för att cybersäkerhetsföretagen har intresse av att rapportera om en viss utveckling, och för att Myndigheten för civilt försvars egna data visar på att andelen leveranskedjeangrepp i inkomna incidentrapporter har minskat från 2023 till 2025.

Not 73. Sveriges Riksbank, *Distributed denial-of-service attacks in the financial sector*, 2025, s. 3–4, 6–7.

Not 74. European Union Agency for Cyber Security, *ENISA Threat Landscape 2022*, 2022, s. 5, 70.

Not 75. CERT-EU, “DDoS Overview and Response Guide”, 2024, hämtad 2025-12-02.

Not 76. Cloudflare, ”Bigger and badder: how DDoS attack sizes have evolved over the last decade”, hämtad 2025-12-02.

Avsnittet behandlar endast en typ av leveranskedjeincident

Myndigheten för civilt försvar delar in leveranskedjeincidenter i två typer: En händelse där något som: (i) ska levereras i den digitala leveranskedjan (en framgångsfaktor eller ett skydd) inte levereras, eller (ii) inte ska levereras i den digitala leveranskedjan (ett hot eller ett hinder) ändå levereras.

Myndighetens bedömning är att aktörerna som står bakom underlagen som myndigheten har analyserat till denna rapport endast behandlar en typ av leveranskedjeincident: incidenter som uppstår på grund av att något som inte ska ha levererats ändå levereras, oftast skadlig kod. Dessa underlag specificerar inte vilken typ av leveranskedjeincident som avses och Myndigheten för civilt försvar har inte heller gjort vidare efterforskningar i detta.

Angrepp mot digitala leveranskedjor kan ha ökat från låg nivå

Andelen cyberangrepp mot leverantörer i incidentrapporter till Myndigheten för civilt försvar under 2025 var få, samtidigt rapporterar andra aktörer om ett ökat antal angrepp mot digitala leveranskedjor.

Andelen cyberangrepp mot leverantörer utgjorde endast 4,5 procent av alla inrapporterade incidenter 2025. Det innebär visserligen en minskning från 2023 och 2024, då leveranskedjeangrepp utgjorde 20 respektive 22 procent av samtliga incidentrapporter, men slutsatser kring trender i leverantörsangrepp bör dras med försiktighet av flera skäl. Som nämnts i avsnittet, Minskning av inrapporterade leverantörsincidenter, har olika angrepp mot digitala leveranskedjor blivit rapporteringspliktiga i olika utsträckning. Därtill rapporterar NIS-leverantörer få angrepp, samtidigt som incidentrapporter från NIS-leverantörer utgör en allt större andel av de totala inkomna incidentrapporterna. Minskningen skulle även kunna bero på ett minskat antal angrepp mot leverantörer hos rapporteringspliktiga verksamhetsutövare, eller en minskad rapporteringsvilja.

Enisas årliga rapporter om cyberhot visar däremot en ökning från 2024 till 2025. Incidenter kopplade till leveranskedjeangrepp utgjorde 10,6 procent av alla angrepp under 2025, jämfört med mindre än två procent under 2024. Det bör även noteras att Enisa presenterar statistik om incidenter kopplade till olika ”hot”, snarare än cyberangrepp, där leveranskedjor utgör en typ av hot.[77]

Samtidigt rapporterar cybersäkerhetsföretag om en ökning av antalet leveranskedjeangrepp i flera avseenden. Cybersäkerhetsföretaget Dragos genomförde till exempel en kartläggning av angrepp från sex hotaktörer som tenderar att angripa

Not 77. European Union Agency for Cyber Security, *ENISA Threat Landscape 2022*, 2022, s. 88; European Union Agency for Cyber Security, *ENISA Threat Landscape 2023*, 2023, s. 4, 127; European Union Agency for Cyber Security, *ENISA Threat Landscape 2024*, 2024, s. 9–10; European Union Agency for Cyber Security, *ENISA Threat Landscape 2025*, 2025, s. 7–9.

ot-system, och konstaterade att det har skett en betydande ökning av deras cyberangrepp mot europeiska leveranskedjor för ot-system från slutet av 2024 och början av 2025. Dragos noterar samtidigt i sina rapporter att slutsatser från analyserna ska dras med försiktighet eftersom det saknas tillräcklig insyn och data inom detta område.[78] Vidare rapporterade cybersäkerhetsföretaget Cyble att cyberangrepp mot leveranskedjor ökade kraftigt under 2025 i jämförelse med 2024, där it-sektorn var mest drabbad.[79]

Även Microsoft har rapporterat att hotaktörer under de senaste åren i allt högre grad har utnyttjat att moderna mjukvarusystem och operativa miljöer ofta är sammanlänkade för att genomföra skadliga aktiviteter, och att kommande år förväntas medföra fler angrepp mot leveranskedjor.[80]

Om leveranskedjeangrepp ökar, kan en anledning vara att organisationers cyberhygien ökar, vilket gör att hotaktörer behöver rikta in sig på leverantörer i leveranskedjan för att genom dem öka sina chanser att nå fler mål. En annan anledning kan vara kriget i Ukraina, då olika källor antyder att angreppen mot ukrainska leveranskedjor och angrepp mot leveranskedjor som kopplas till kriget har ökat, se nedan.

Enligt cybersäkerhetsorganisationen RCDC förekom ryska angrepp mot leveranskedjor frekvent under 2024 och 2025.[81] Enligt en ukrainsk myndighet har antalet cyberangrepp i Ukraina som riktas direkt mot kritisk infrastruktur minskat till förmån för indirekta angrepp mot infrastrukturens leverantörskedjor och utvecklare av specialiserad programvara.[82] Bland annat skriver Enisa att hotaktörer som kan kopplas till Ryssland har riktat in sig på ukrainska och europeiska leveranskedjor för vapen och humanitärt bistånd.[83] Därtill avslöjade brittiska myndigheter i maj 2025 att Rysslands säkerhetstjänst har bedrivit en cyberoperation mot västerländska logistik- och teknikföretag sedan 2022.[84]

Fysiska komponenter kan påverka digitala leveranskedjor

Säkerheten i digitala leveranskedjor kan även påverkas av hårdvaran, där brist på eller hot inom hårdvarukomponenter kan påverka kommunikationssystem eller digital infrastruktur. Hotaktörer i leveranskedjan kan exempelvis leverera

Not 78. Dragos, *9th Annual 2026 Year in Review*, 2026, s. 36.

Not 79. Cyble bedömer leveranskedjeangrepp utifrån omnämningar som gjorts av hotaktörer på Darknet. I och med att omnämningarna kommer från hotaktörerna själva ska de tolkas med försiktighet.

Not 80. Microsoft, *Microsoft Digital Defense Report 2025*, 2025, s. 14.

Not 81. The Regional Cyber Defence Centre, *A Comparative Study of Russian Offensive Cyber Capabilities*, 2025, s. 32.

Not 82. State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force, *War And Cyber: Three Years Of Struggle And Lessons For Global Security – Analytical Report*, Kyiv, 2025, s. 12.

Not 83. NSA genom Enisa: European Union Agency for Cyber Security, *ENISA Threat Landscape 2023*, 2023, s. 124.

Not 84. National Cyber Security Centre of UK, "UK and allies expose Russian intelligence campaign targeting western logistics and technology organisations", hämtad 2025-11-18; National Cyber Security Centre of UK, *NCSC Annual review 2024*, 2024.

en komprometterad hårdvara som tillåter obehörig åtkomst eller fjärrstyrning.[85] Under 2024 uppdagades att personsökare, inköpta av Hizbollah i Libanon från en leverantör i Taiwan, hade blivit komprometterade med ett svårupptäckt sprängämne av en underleverantör i Europa. Sprängämnet kunde fjärraktiveras via krypterade meddelanden och detonera kort därefter. Personsökarna hade tidigare identifierats av angriparen som ett möjligt sätt att penetrera den libanesiska gruppens kommunikationssystem.[86] CNN skriver att angreppet kan ha syftat till att skapa paranoia inom gruppen, försvåra rekrytering och underminera förtroendet för gruppens förmåga att skydda sina medlemmar.[87]

Ett ytterligare exempel på en komprometterad hårdvara är kinesiska växelriktare som används i solcellsparker i USA och Europa. I maj 2025 rapporterade The Times att otillåtna dolda mobilradiomoduler[88], hade upptäckts i kinesiska växelriktare i solcellsparker i USA och Europa. Upptäckten tyder på att angripare skulle kunna fjärraktivera enheterna för att stänga av eller skada växelriktarna på distans.[89] Därför är det viktigt att leverantörer kommunicerar med sina underleverantörer och ser över vilka komponenter som finns i de produkter som köps in.

Indikationer på att antalet angrepp mot ot-system har ökat

Flera aktörer har rapporterat om att cyberangrepp mot ot-system har ökat de senaste åren.[90] Det handlar exempelvis om ett ökat antal utpressningsangrepp mot ot-system och en intensifiering av angrepp mot vissa sektorer. De sektorer som främst uppges ha varit drabbade av angrepp mot ot-system är tillverkningsindustrin, följt av transportsektorn och industriella system, som är en typ av ot-system. Rapporterna redogör även för att många angrepp har skett inom ramen för, eller har motiverats av, pågående geopolitiska konflikter.

Dessa rapporter kommer i huvudsak från privata företag som säljer olika cybersäkerhetstjänster, men Myndigheten för civilt försvar bedömer att rapporterna ger en indikation om utvecklingen inom området. Anledningen är att den observerade trenden både följer utvecklingen i cyberkrigföringen, där antalet angrepp mot

Not 85. Myndigheten för samhällsskydd och beredskap, *Hoten mot de digitala leveranskedjorna*, 2021, s. 23, 42.

Not 86. The Guardian, ”Hezbollah device blasts: how did pagers and walkie-talkies explode and what do we know about the attacks?”, hämtad 2026-01-09.

Not 87. CNN,”How did pagers explode in Lebanon and why was Hezbollah using them? Here’s what we know”, hämtad 2026-01-09.

Not 88. En typ av mobilradio som möjliggör omedelbar röst- och datakommunikation över mobilnätverk.

Not 89. The Times, “Chinese ‘kill switches’ found hidden in US solar farms”, hämtad 2026-01-08.

Not 90. Dragos, *9th Annual 2026 Year in Review*, 2026; Waterfall Security, *OT Cyber Threat Report 2025*, 2025; European Union Agency for Cyber Security, *Enisa Threat Landscape 2025*, 2025; The Regional Cyber Defence Centre, *A Comparative Study of Russian Offensive Cyber Capabilities*, 2025; Ministry of Foreign Affairs of Ukraine, ”Joint Statement on Russia’s deliberate attacks against Ukraine’s civilian energy infrastructure”, hämtad 2025-12-02.

ot-system och kritisk infrastruktur har ökat både i Ukraina och i länder som stödjer Ukraina i kriget, och för att den stämmer överens med myndighetens analys av flera noterbara angrepp mot ot-system de senaste åren. Sett till denna utveckling bedömer även Myndigheten för civilt försvar att geopolitiska spänningar skulle kunna vara en anledning till att angreppen mot ot-system har ökat under perioden.

Kort om ot-system

System för operativ teknik, ot-system, lagrar och bearbetar information samt reglerar fysiska styrsystem, ofta med direkt påverkan på människa eller omgivning.[91] Det kan till exempel handla om styrsystem för kollektivtrafik, produktion av kraftvärme, dricksvattensystem och skyddsdörrar.

Traditionellt sett har ot-system varit fysiskt isolerade och byggt på specialutvecklad teknik, men i takt med den tekniska utvecklingen har gränserna mellan ot-system och informationssystem, it-system, blivit mindre tydliga.[92] När it- och ot-system integreras uppstår nya risker. Industriella ot-system kan exempelvis göras tillgängliga för angrepp via it-system. Ett cyberangrepp mot ett ot-system kan få stora konsekvenser, både ur ett ekonomiskt perspektiv och ett personskadeperspektiv eftersom angreppet kan påverka både verksamhet och människor.[93]

Flera rapporterar om en ökning av antalet angrepp mot ot-system

Enligt cybersäkerhetsföretagen Dragos och Waterfall Security[94] har cyberangrepp mot ot-system ökat globalt under de senaste åren. Dragos redovisade år 905 utpressningsangrepp mot ot-system 2023, 1 693 angrepp år 2024 och 3 318 angrepp år 2025.[95] Företagen kopplar angrepp mot ot-system till geopolitiska spänningar.[96] Därtill anger företagen att det har skett en ökning mot vissa sektorer. Det handlar främst om tillverkningssektorn följt av transportsektorn och industriella styrsystem, men gäller även sektorer inom olja och gas, energi, och mot statliga

Not 91. Myndigheten för samhällsskydd och beredskap, *Undersökning om ot-säkerhet*, [Elektronisk resurs] 2025, s. 5.

Not 92. Myndigheten för civilt försvar, ”Cyberfysiska system – en introduktion”, hämtad 2026-03-20.

Not 93. Myndigheten för samhällsskydd och beredskap, *Ökad säkerhet i industriella informations- och styrsystem*, 2021, s. 17.

Not 94. Waterfall Security inkluderar bara incidenter som är avsiktliga, som medför fysiska konsekvenser, som påverkat tillverkning, industri, infrastruktur och transport, och som offentliggjorts. Många incidenter har uteslutits av företaget på grund av sekretess, misstro till äkthet eller brist på tillgång till rapporter på vissa språk.

Not 95. Dragos, *9th Annual 2026 Year in Review*, 2026, s. 65; Dragos, *8th Annual Year in Review 2025*, 2025, s. 39; Dragos, *OT Cybersecurity the 2023 Year in Review*, 2024, s. 23.

Not 96. Waterfall Security, *OT Cyber Threat Report 2025*, 2025, s. 9; Dragos, *9th Annual 2026 Year in Review*, 2026, s. 18; Dragos, *8th Annual Year in Review 2025*, 2025, s. 35.

aktörer.[97] Tillverkningsindustrin är den mest drabbade sektorn och står för mer än hälften av de observerade utpressningsangreppen under de senaste åren. Antalet angrepp mot sektorn ökade från 638 under 2023 till 2 259 under 2025.[98]

Även Enisa rapporterade 2025 att ot-system och kritisk infrastruktur utsätts för allt fler och mer avancerade cyberangrepp. Enisa skriver att ot-relaterade hot står för drygt 18 procent av de observerade angreppen under perioden.[99]

Flera europeiska länder drabbade av angrepp mot ot-system

Enisa bedömer att europeiska ot-system och kritisk infrastruktur är fortsatt måltavlor för cyberangrepp, med hänvisning till angrepp som har skett inom EU. Hotaktörer har exempelvis angripit internetåtkomliga ot-system som styr energi- och vattenkraftverk inom flera europeiska länder, där Italien, Tjeckien, Frankrike och Spanien varit mest drabbade. Även om angreppen inte hade någon betydande påverkan på den operativa verksamheten bedömde Enisa att syftet var att skapa psykologisk påverkan.[100]

Myndigheten för civilt försvar har i sin analys även uppmärksammat ett antal angrepp mot ot-system i såväl Norden, som övriga Europa under 2025. Ett cyberangrepp mot en damm i Norge april 2025 genomfördes enligt Politiets sikkerhetstjeneste (PST) för att påverka opinionen och skapa oro. PST noterade att cyberangrepp mot västerländsk infrastruktur ökar och sannolikt kommer fortsätta öka både i Norge och andra europeiska länder.[101] I december 2025 uppgav även Danmarks militära underrättelsetjänst (FE) att en hotaktör, med koppling till Ryssland, låg bakom ett cyberangrepp mot ett vattenverk vid staden Køge, vilket påverkade vattentrycket och ledde till att ledningar sprack och att hushåll blev utan vatten under en oklar tidperiod.[102]

Även Polen utsattes i december 2025 för flera cyberangrepp mot ot-system kopplade till landets elförsörjning, vilka var nära att orsaka ett strömavbrott. Den polska energiministern uppgav att incidenten skiljde sig från tidigare angrepp då flera mindre anläggningar nu angreps parallellt, och att Polen kan förvänta sig liknande angrepp framöver. Enligt den polska digitaliseringsministern

Not 97. Dragos, *9th Annual 2026 Year in Review*, 2026, s. 65; Dragos, *8th Annual Year in Review 2025*, 2025, s. 39; Dragos, *OT Cybersecurity the 2023 Year in Review*, 2024, s. 23; Waterfall Security, *OT Cyber Threat Report 2025*, 2025, s. 11.

Not 98. Dragos, *9th Annual 2026 Year in Review*, 2026, s. 65; Dragos, *8th Annual Year in Review 2025*, 2025, s. 39; Dragos, *OT Cybersecurity the 2023 Year in Review*, 2024, s. 23; Dragos, *ICS/OT Cybersecurity Year in Review 2022*, 2023, s. 4, 31.

Not 99. European Union Agency for Cyber Security, *Enisa Threat Landscape 2025*, 2025, s. 8.

Not 100. European Union Agency for Cyber Security, *Enisa Threat Landscape 2025*, 2025, s. 53–54.

Not 101. Verdens Gang, ”PST-sjefen: Mener russere sto bak norsk dam-sabotasje”, hämtad 2025-12-02; Norsk Rikskringkasting, ”PST: Mener russere sto bak norsk dam-sabotasje”, hämtad 2025-12-02.

Not 102. Dagens Nyheter, ”Danmark pekar ut Ryssland för cyberangrepp”, hämtad 2026-01-13.

pekade angreppen på ryskt sabotage.[103] En samlad rapport om incidenten från Polens nationella cybersäkerhetsorgan, CERT-PL uppgav att det var värt att notera att angreppet genomfördes samtidigt som Polen hade kämpat med låga temperaturer och snöstormar.[104] Angreppets karaktär utgjorde en noterbar eskalering i jämförelse med tidigare incidenter i Polen, enligt CERT-PL.[105]

Angrepp mot ot-system med koppling till geopolitik

Cybersäkerhetsorganisationen RCDC rapporterar hur Ryssland sedan 2022 i allt större utsträckning har riktat in sig på ot-system kopplade till kritisk infrastruktur i Ukraina. Denna utveckling började bland annat med angreppet mot Ukrainas elnät i april 2022. RCDC menar att ryska hotaktörer därefter har testat och utvecklat ny skadlig kod specifikt för industriella styrsystem, där ett exempel är den skadliga koden COSMICENERGY, som utformats för att skicka falska kommandon till fjärrterminalenheter med syfte att orsaka strömavbrott.[106] Ukrainas utrikesdepartement har uppgett att landets energisektor har utgjort ett mål för ryska cyberangrepp och att dessa angrepp har intensifierats under det senaste året.[107] I november 2025 utsattes exempelvis Ukrainas energisektor för ryska drönarangrepp, vilket ledde till omfattande skador på energianläggningar i flera regioner och strömavbrott.[108]

RCDC rapporterar även att Rysslands fokus på kritisk infrastruktur har sträckt sig bortom Ukraina och riktats mot västerländska system i länder som stödjer Ukraina. Under 2022–2023 genomfördes kampanjer mot energi-, transport- och rörledningssystem i flera NATO-länder.[109]

Cyberangrepp kan vara ett medel för cyberspionage och informationspåverkan

Erfarenheter från kriget i Ukraina har visat att cyberangrepp kan användas för cyberspionage, sabotage och informationspåverkan. Avsnittet redogör för att cyberangrepp är ett verktyg för cyberspionage och informationspåverkan och att det finns en risk för incidenter samt påverkansaktiviteter via cyberangrepp mot Sverige, bland annat mot den svenska valprocessen under 2026.

Not 103. The Record, “Poland says it repelled major cyberattack on power grid, blames Russia”, hämtad 2026-02-12.
Not 104. CERT-PL, ”Energy Sector Incident Report – 29 December 2025”, 27 februari 2026.
Not 105. Ibid.
Not 106. The Regional Cyber Defence Centre, *A Comparative Study of Russian Offensive Cyber Capabilities*, 2025, s. 24.
Not 107. Ministry of Foreign Affairs of Ukraine, ”Joint Statement on Russia’s deliberate attacks against Ukraine’s civilian energy infrastructure”, hämtad 2025-12-02.
Not 108. Government of the United Kingdom, ”Russia’s attacks on Ukraine’s energy infrastructure deepen humanitarian harm and endanger nuclear safety: UK statement to the OSCE”, hämtad 2025-12-02.
Not 109. The Regional Cyber Defence Centre, A Comparative Study of Russian Offensive Cyber Capabilities, 2025, s. 24.

Cyberspionage är ett hot inom och utanför cyberkrigföring

Erfarenheter från kriget i Ukraina har visat att cyberspionage kan få allvarliga konsekvenser för så väl samhällsfunktioner som för militära mål. Cyberspionage kan användas för att etablera en långsiktig närvaro i system med syfte att leverera underrättelser för att kunna stödja framtida cyberangrepp.

Rapporter från myndigheter i Ukraina antyder att Rysslands cyberspionage har ökat under 2024.[110] Därtill har både Enisa och Microsoft i separata analyser uppgett att statliga aktörer har intensifierat sitt cyberspionage under 2024 och 2025. Det handlar både om en ökning av cyberspionage för att komplettera traditionella underrättelseoperationer,[111] samt om att det under en längre tid har förekommit cyberspionage inom EU under 2025.[112]

Enisa bedömer att cyberspionage utgör en mindre andel av cyperoperationer som härleds till statliga aktörer. Samtidigt pekar Enisa på att cyberspionage kan ta lång tid att upptäcka, och relaterade incidenter dokumenteras ofta först efter 6 månader till över 4 år, vilket gör det svårt att uppskatta den verkliga omfattningen. Enisas bedömning är att cyperspionage fortsatt är ett viktigt hot, och att EU-organisationer kan väntas utsättas för cyberspionage från aktörer med koppling till Kina och Ryssland i närtid.[113]

Många gånger har cyberspionage skapat en långsiktig närvaro för att kunna leverera underrättelser, eller för att plantera skadlig kod för att utföra angrepp vid ett senare tillfälle.[114] Redan 2018 bedrev Ryssland cyberspionage i ukrainska nätverk som sedan utnyttjades i de omfattande och destruktiva cyberangreppen under den fullskaliga invasionen av Ukraina, och Ukraina har fortsatt utsatts för cyberspionage av Ryssland sedan dess.[115] CERT-UA har rapporterat om en ökning av spionageoperationer sedan 2024, där operationerna inte bara riktat in sig mot statliga aktörer utan även mot andra sektorer, vilket tyder på att Rysslands underrättelseverksamhet har blivit alltmer omfattande.[116] Spionage har även

Not 110. State Service of Special Communications and Information Protection of Ukraine, *Russian Cyber Operations – Analytics for the H2 2024*, 2024, s. 11; Vasylieva, T., Yarovenko, H., & Zakharkin, O., *Digital Transformations of Ukraine's Cybersecurity System in Wartime*, 2025, s. 45.

Not 111. Microsoft, *Microsoft Digital Defense Report 2025*, s. 5.

Not 112. European Union Agency for Cyber Security, *ENISA Threat Landscape 2025*, 2025, s. 6, 36, 63.

Not 113. Ibid.

Not 114. Se till exempel angreppet 2023 mot Ukrainska mediebolag: BleepingComputer, "Ukraine: Sandworm hackers hit news agency with 5 data wipers", hämtad 2026-02-27; samt angreppet mot Ukrainska myndigheter 2023 som påbörjades 2021 med installationen av bakdörrar: CERT-UA, "Кібератака, спрямована на порушення цілісності та доступності державних інформаційних ресурсів (CERT-UA#6060)", hämtad 2026-02-27.

Not 115. Totalförsvarets forskningsinstitut (FOI), *Unraveling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)*, 2023, s. 38.

Not 116. State Service of Special Communications and Information Protection of Ukraine, *Russian Cyber Operations – Analytics for the H2 2024*, 2024, s. 11; Vasylieva, T., Yarovenko, H., & Zakharkin, O., *Digital Transformations of Ukraine's Cybersecurity System in Wartime*, 2025, s. 45.

utförts inom underrättelseoperationer för att samla in känslig information som kunde stödja militära insatser på marken.[117]

Även Sverige utsätts för cyberspionage av främmande makt, enligt Försvarets radioanstalt (FRA) som bedömer att Ryssland, Kina och Iran är de länder som främst hotar Sveriges säkerhet.[118] Dessa stater bedriver spionage mot Sverige, varav metoderna inkluderar cyberangrepp, påverkansoperationer och sabotage.[119] Spionage bedrivs exempelvis mot svensk försvarsindustri och myndigheter i syfte att kartlägga Sveriges försvarsförmåga och sårbarheter.[120] Den vanligaste formen av främmande underrättelseverksamhet mot Sverige utgörs enligt FRA idag av angrepp mot it-system, även om traditionella metoder också förekommer.[121]

Cyberangrepp är ett verktyg för informationspåverkan

Erfarenheter från cyberkrigföringen mellan Ryssland och Ukraina visar att cyberangrepp oftast används som ett verktyg för informationspåverkan.[122]

Totalförsvarets forskningsinstitut (FOI) menar i en rapport om cyberkriget i Ukraina att Rysslands cyberangrepp varit en möjliggörare av informationspåverkan och att Rysslands strategi att kontrollera informationsmiljön inte varit ett totalt misslyckande.[123] Enligt aktörer var informationspåverkansangrepp mot Ukraina frekvent förekommande under 2022 och 2023.[124] Cyberangreppen sträckte sig från SMS-kampanjer till angrepp mot tv-stationer och intrång till sociala mediekonton.[125] ENISA redogör exempelvis för att desinformation i form av deepfakes spelade en viktig roll i Rysslands fullskaliga invasion av Ukraina då det bland annat resulterade i en spridning av falska videor på Rysslands president Vladimir Putin och Ukrainas president Volodymyr Zelenskyj med budskap som stödde motståndarnas åsikter.[126]

Not 117. The Regional Cyber Defence Centre, *A Comparative Study of Russian Offensive Cyber Capabilities*, 2025, s. 19.

Not 118. Försvarets radioanstalt, *FRA Årsrapport 2024 – Utmanande och Komplex Hotbild*, 2025, s. 4.

Not 119. Försvarsmakten, ”Hybridoperationer skadar Sverige”, hämtad 2025-11-07.

Not 120. Försvarets radioanstalt, *Cybersäkerhet i Sverige 2024*, 2025, s. 4.

Not 121. Försvarets radioanstalt, ”Hybridhot”, hämtad 2025-11-07.

Not 122. Informationspåverkan avser information som är medvetet vilseledande, har för avsikt att störa den offentliga debatten, och stör och försvagar samhället. Se Myndigheten för psykologiskt försvar, ”Informationspåverkan och val”, hämtad 2025-12-02.

Not 123. Totalförsvarets forskningsinstitut (FOI), *Unraveling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023),* 2023.

Not 124. State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force, *War And Cyber: Three Years Of Struggle And Lessons For Global Security – Analytical Report*, Kyiv, 2025; The Regional Cyber Defence Centre, *A Comparative Study of Russian Offensive Cyber Capabilities*, 2025.

Not 125. Cyber Peace Institute, ”Ukraine: Beyond Kinetics”, hämtad 2025-11-11.

Not 126. European Union Agency for Cyber Security, *ENISA Threat Landscape 2022*, 2022.

Försvarsmakten menar att Sverige utgör ett av målen i Rysslands strategi att underminera västvärldens enighet, där påverkansoperationer är ett centralt medel.[127] Enligt Säkerhetspolisen finns det risk för sabotage och incidenter samt påverkansaktiviteter via cyberangrepp från Ryssland riktat mot västs stöd till Ukraina.[128] Säkerhetspolisen räknar även med att Ryssland kan försöka påverka den svenska valprocessen under 2026, samtidigt som Säkerhetspolisen betonar att Sverige har ett stabilt valsystem som ska klara av cyberangrepp.[129]

Ett exempel på informationspåverkan i samband med val kommer från det Norska Forsvarets forskningsinstitutt (FII) som har analyserat påverkan i samband med det norska valet 2025. FII bedömde att hotaktörer kombinerade överbelastningsangrepp mot bland annat partihemsidor i samband med påverkanskampanjer på sociala medier.[130]

Cyberangrepp används mer i samband med kinetiska angrepp i cyberkrigföringen

Cyberangrepp kan vara ett effektivt verktyg i krigföring. Cyberangrepp kan medföra stora kostnader, skapa förseningar och utgöra allmänna störningar för samhället och försvarsförmågan.[131] Samtidigt är det svårt att dra slutsatser om konsekvenserna av cyberangreppen i kriget i Ukraina.

I början av Rysslands fullskaliga invasion av Ukraina var det till exempel få, om några, cyberoperationer som hade liknande påverkan som de kinetiska angreppen.[132] En anledning till det är att Ukrainas cyberförsvar bedöms vara mycket starkt, vilket sannolikt har avvärjt större konsekvenser på samhällsnivå.[133] Det är dessutom svårt att få information om de militära effekterna av cyberangrepp via öppna källor, på grund av de intressen som ligger bakom vilken information som delas. Det går dock att konstatera att de ryska cyberangreppen mot Ukraina inte har lett till så stora konsekvenser som många förväntade sig.[134]

Not 127. Försvarsmakten, *Säkerhetsläget i Närområdet,* hämtad 2025-11-07.

Not 128. Säkerhetspolisen, ”Fortsatt förhöjd terrorhotnivå i allvarligt säkerhetsläge”, hämtad 2026-01-16.

Not 129. Expressen, ”Säpo mobiliserar mot rysk valpåverkan”, hämtad 2026-01-16.

Not 130. FII, ”Økende, komplekst og uoversiktlig – kartlegging av utenlandsk påvirkning i forbindelse med stortingsvalget 2025” Norwegian Defence Research Establishment, hämtad 2026-02-27.

Not 131. Myndigheten för samhällsskydd och beredskap, *När kriget kom nära*, 2023, s. 42.

Not 132. Totalförsvarets forskningsinstitut (FOI), *Unraveling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)*, 2023, s. 3.

Not 133. Se Myndigheten för samhällsskydd och beredskap, *När kriget kom nära*, 2023.

Not 134. Totalförsvarets forskningsinstitut (FOI), *Unraveling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)*, 2023, s. 3; CNN, ”Russia’s cyber offensive against Ukraine has been limited so far. Experts are divided on why”, hämtad 2025-11-12.

Det är i stället cyberangrepp i kombination med kinetiska, eller fysiska, angrepp som cyberangrepp är mest effektiva i krigföringen.[135] Sedan krigets inledande fas har det skett en utveckling mot mer och mer koordinerade angrepp i cyber- och den kinetiska sfären. Tidigare kunde cyberangrepp bestå av korta och destruktiva operationer, så som angreppen mot Ukrainas telenät under 2022 och 2023,[136] medan cyberangrepp under de senare åren snarare utgör en beståndsdel av en större strategi.[137] Under den senare delen av 2022 började Ryssland oftare använda cyberangrepp mot energiinfrastruktur som förberedelse för efterföljande missilangrepp.[138]

Sedan krigets inledande fas har även kinetiska angrepp skett i kombination med påverkansoperationer och cyberangrepp.[139] Det förekommer även exempel på kinetiska angrepp med hjälp av intrång i IoT-enheter,[140] så som ukrainska soldaters mobiltelefoner, smartklockor och surfplattor. Avsikten har varit spionage, eller att komma åt meddelanden som rör militära planer.[141] I ett fall hackades en soldats smartklocka, vilket ledde till att ryska hackare fick tillgång till soldatens meddelanden via applikationen Signal. Åtkomsten till känslig information gjorde det möjligt att utföra ett kinetiskt angrepp mot platsen där soldatens trupp befann sig.[142]

Not 135. Totalförsvarets forskningsinstitut (FOI), *Unraveling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)*, 2023, s. 3.

Not 136. Under 2002–2023 drabbades Ukraina av ett flertal destruktiva cyberangrepp mot bland annat telekomindustrin. Under den fullskaliga invasionens första dag drabbades Viasats satellitbaserade KA-SAT-nätverk av ett leveranskedjeangrepp vilket slog ut åtkomsten till internet för fler än 500 000 bredbandskunder i centrala Europa i upp till två veckor, se Myndigheten för samhällsskydd och beredskap, *När kriget kom nära,* 2023. Under våren 2023 drabbades elva telekombolag i Ukraina av dataintrång som ledde till avbrott i teletjänster för befolkningen, se Bleeping Computer, ”Russian Sandworm hackers breached 11 Ukrainian telcos since May”, 2023-10-16, hämtad 2025-11-28.

Not 137. The Regional Cyber Defence Centre, *A Comparative Study of Russian Offensive Cyber Capabilities*, 2025, s. 8–9.

Not 138. Ibid, s. 27.

Not 139. Ibid.

Not 140. Internet of Things, eller IoT är ett begrepp som används för att beskriva att allt fler föremål, både för privat- och industriellt bruk, utrustas med möjligheten att anslutas till internet och andra nätverk.

Not 141. Se till exempel Forbes, ”Russia Is Targeting Ukrainian Soldiers’ Signal Accounts, Google Warns”, hämtad 2025-11-12; CNN, ”Russian military hackers take aim at Ukrainian soldiers’ battle plans, US and allies say”, hämtad 2025-11-12.

Not 142. Representanter för State Service of Special Communications and Information Protection of Ukraine (SSSCIP). *Kriget i Ukraina – erfarenheter och insikter kopplat till cyberarenan – panelsamtal, Cybersäkerhetskonferensen 2025*. [Webbinspelning]. Myndigheten för civilt försvar, 2026, hämtad 2026-02-25.

Slutsatser och rekommendationer

Slutsatser och rekommendationer

I detta avsnitt presenterar myndigheten för civilt försvar de centrala slutsatser och rekommendationer som har dragits från årsrapporten i sin helhet. För fördjupad läsning hänvisar myndigheten till avsnitten i kapitlen ovan, samt tidigare rapporter.

Hotaktörer utvecklar kontinuerligt sin cyberangreppsförmåga

Trots att incidentrapporterna som inkommit till Myndigheten för civilt försvar visar att andelen inrapporterade cyberangrepp har minskat under 2025, uppger källor som myndigheten har analyserat att det har skett en utveckling av cyberangrepp under 2023 till 2025. Avsnitten i temakapitlet har redogjort för att vissa typer av angrepp har ökat under vissa perioder, och mot vissa sektorer, att vissa angrepp har effektiviserats med hjälp av AI, och att vissa angrepp, så som vissa överbelastningsangrepp, har blivit mer omfattande och svårhanterliga. Sammantaget drar Myndigheten följande övergripande slutsatser: hotaktörer utvecklar kontinuerligt sin cyberangreppsförmåga, tillämpar flera olika angreppsmetoder, och angriper olika sektorer.

Eftersom hotaktörer fortsätter att utveckla och effektivisera sina metoder, samt använder sig av olika typer av angrepp mot mål i olika sektorer, behöver samhällsviktiga verksamhetsutövare kontinuerligt stärka sin motståndskraft. Sveriges förmåga att upprätthålla samhällsviktiga funktioner vid cyberangrepp och krigsrisk kommer att avgöras av hur väl organisationer har arbetat systematiskt med sitt cybersäkerhetsarbete. Det är genom ett systematiskt och riskbaserat cybersäkerhetsarbete som incidenter kan förebyggas och en förmåga att motstå cyberangrepp upprättas. Enligt resultatet från Cybersäkerhetskollen 2025, ett verktyg hos Myndigheten för civilt försvar som bedömer nivån på cybersäkerhetsarbetet hos svenska organisationer, finns det allvarliga brister i det systematiska cybersäkerhetsarbetet hos offentlig förvaltning. Samhällsviktiga verksamhetsutövare behöver därför höja nivån på sitt cybersäkerhetsarbete.[143]

Not 143. Myndigheten för civilt försvar, Cybersäkerhetskollen 2026, *Redovisning av uppföljning av nivån på det systematiska cybersäkerhetsarbetet i offentlig förvaltning och samhällsviktig verksamhet*, 2026, hämtad 2026-03-02.

Rekommendationer

- Utveckla, prioritera och resurssätt det systematiska och riskbaserade cybersäkerhetsarbetet.
- Använd Myndigheten för civilt försvars och Nationellt cybersäkerhetscenters stöd och verktyg för att utveckla cybersäkerhetsarbetet, samt följ myndigheternas rekommendationer för hur verksamheter kan förebygga och hantera olika angrepp.[144]

Incidentrapporteringen måste förbättras

Kapitlet om inkomna incidentrapporter redogör för Myndigheten för civilt försvars bedömning att det finns ett stort mörkertal avseende antalet inkomna incidentrapporter. Därtill rapporteras en stor andel incidenter ha okänd orsak, samtidigt som fritextsvaren visar att orsaken är känd. Andelen incidentrapporter som anger okänd orsak har ökat från 12 procent år 2022, till 31 procent år 2025. Att andelen ökar kan bero på att andelen incidentrapporter som rapporteras av NIS-leverantörer ökar, och det företrädelsevis är NIS-leverantörer som rapporterar okänd orsak.

Felrapportering kan bero på okunskap hos anmälaren eller otydligheter i Myndigheten för civilt försvars stöd eller verktyg för inrapportering. Myndigheten kan inte med säkerhet bedöma vad utvecklingen beror på, men arbetar för närvarande med ett nytt verktyg för inrapportering i enlighet med den nya cybersäkerhetslagen, och kommer att se över aktuella stöd för inrapportering.

Mörkertalen och felrapporterade incidenter begränsar Myndigheten för civilt försvars förmåga att skapa en helhetsbild av nuläget och utvecklingen över tid. Det underminerar även förmågan att ta fram ändamålsenligt stöd till verksamhetsutövare. Det är därför en grundförutsättning att verksamhetsutövare lyder rapporteringsplikten för att motståndskraften i det civila försvaret ska kunna öka. Om samhällsviktiga verksamhetsutövare kan hitta bättre arbetssätt för att identifiera varför incidenter uppstår och vilka sårbarheter som kan föranleda dessa, står de bättre rustade om angrepp inträffar.

Rekommendationer

- Stärk arbetssätten för incidentrapportering för att få en bättre förståelse för varför incidenter drabbar den egna verksamheten och bidra till Sveriges motståndskraft.

Not 144. Se lista över Myndigheten för civilt försvars tillgängliga stöd och verktyg i Myndigheten för samhällsskydd och beredskap, *Verktyg för ökad motståndskraft och stärkt civilt försvar*, 2025.

Många angrepp har en koppling till geopolitik

Flera av de källor myndigheten har analyserat har visat på att cyberangrepp ofta har en geopolitisk koppling. Det har exempelvis utförts överbelastningsangrepp i samband med val, i samband med Sveriges och Finlands inträden i Nato, angrepp mot ot-system i pågående geopolitiska konflikter, samt leveranskedje-angrepp mot ukrainska och europeiska leveranskedjor för vapen och humanitärt bistånd. Erfarenheter från anfallskriget i Ukraina har även visat att cyberangrepp ofta används som ett verktyg för informationspåverkan. Mot bakgrund av denna utveckling bedömer myndigheten att cyberangrepp i Sverige kan öka i samband med utrikespolitiska ställningstaganden eller i samband med val, bland annat med syftet informationspåverkan.

Givet att många angrepp har en koppling till geopolitik behöver samhällsviktiga verksamhetsutövare jobba systematiskt med att identifiera både interna och externa risker och hot, vilket kräver omvärldsbevakning av incidenter och angreppsmetoder. En aktiv omvärldsbevakning ökar verksamheters förståelse för potentiella hot och sårbarheter som kan påverka verksamheten, vilket på sikt bidrar till ett stärkt civilt försvar.

Rekommendationer

- Bedriv omvärldsbevakning för att identifiera risker, som hot och sårbarheter.[145]

Not 145. Omvärldsbevakningen bör samla information från leverantörer av organisationens hårdvara och mjukvara, Sveriges nationella CSIRT, expert- och tillsynsmyndigheter, källor som bevakar den övergripande utvecklingen av ny teknik på it-området.

Framåtblick

Framåtblick

Den 15:e januari 2026 trädde cybersäkerhetslagen i kraft. Det är en epokgörande ny lagstiftning med omfattande implikationer på cybersäkerhetsarbetet i Sverige. En av flera särskilt viktiga aspekter är att antalet organisationer som omfattas av cybersäkerhetslagen utökas kraftigt jämfört med innan. Myndigheten för civilt försvar bedömer att 2 000 eller fler organisationer omfattas av cybersäkerhetslagen och att den stora majoriteten av dessa är privata bolag. Detta kan jämföras mot omkring 600 bolag som tidigare omfattades av NIS-lagstiftningen.

Givet att antalet rapporteringspliktiga organisationer kraftigt utökas borde fler incidentrapporter inkomma under 2026. Cybersäkerhetslagen innebär även en utökning av vilken typ av information som kan inrapporteras. Incidentrapporteringen ska nämligen kompletteras med möjligheten att inrapportera cyberhot, tillbud och sårbarheter.

I skrivande stund och vid tillfället för denna rapports publicering nyttjas en interimslösning för incidentrapporteringen. Under andra kvartalet 2026 kommer de nya föreskrifterna för cybersäkerhetslagen börja gälla och då kommer även nya formulär för incidentrapportering, cyberhot, tillbud och sårbarheter att lanseras.

Den 1 juli 2026 kommer Myndigheten för civilt försvars samlade utåtriktade cyberuppdrag föras över till Försvarets radioanstalt och införlivas i Nationellt cybersäkerhetscenter (NCSC). NCSC kommer i samband med detta att formellt ta över ansvaret för den datainhämtning som denna rapport bygger på. Nästa årsrapport kommer följdriktigt att publiceras av NCSC.

Myndigheten
för civilt försvar