NISCHOMRÅDE · KURERAD TRENDANALYS

Strategier för desinformationshantering och valintegritet

Expertstöd för organisationer och myndigheter att hantera desinformation och skydda valintegriteten inför framtida demokratiska processer.

UPPDATERAD 1 augusti 2026

Mikro Makro Mega

11
PUBLICERADE TRENDER

KORT SVAR

Det viktigaste i analysen

Organisationer och myndigheter måste stärka sin beredskap mot desinformation genom **proaktiv kriskommunikation** och formaliserad samverkan. AI-drivna påverkansoperationer och deepfakes kräver omedelbara åtgärder som **standardiserade incidentrutiner** och teknisk verifiering inför valåret 2026.

01 Hur bör ledningen prioritera resurser för att skydda organisationen mot utländsk informationspåverkan och desinformation?

Ledningen bör prioritera att integrera desinformation i befintliga risk- och sårbarhetsanalyser samt etablera **strukturerade ramverk för psykologiskt försvar**. Samarbeten mellan offentlig och privat sektor genom **nationella beredskapsnätverk** blir avgörande för att dela hotbilder.

02 Vilken strategi är mest effektiv för att möta snabbt spridda deepfakes och AI-genererade rykten under en valrörelse?

Genom att tillämpa **proaktiv kriskommunikation** kan organisationer förutse narrativ innan de får fäste. Detta bör kombineras med **AI-baserade verifieringsverktyg** för att snabbt upptäcka manipulerat innehåll.

03 Vilka risker innebär den ökade spridningen av AI-driven desinformation för organisationers finansiella stabilitet och varumärke?

Falska rykten utgör direkta hot mot ekonomin och kan skada organisationens anseende i stor skala, vilket bekräftas av att **generativ AI förändrar spelplanen** och gör det billigt att producera övertygande desinformation.

04 Vilka investeringar i teknik och system krävs för att möta de nya kraven på incidentrapportering inför valet 2026?

Organisationer behöver implementera **digitala system för incidentrapportering** samt göra **resiliensbaserade riskbedömningar** av den digitala infrastrukturen.

MAKROTREND

Stärkt samverkan mellan offentlig och privat sektor för valintegritet

En ökad formalisering av samarbeten mellan myndigheter och digitala plattformar/företag för att säkra informationsmiljön. Detta innebär att organisationer i allt högre grad förväntas delta i nationella beredskapsnätverk för att motverka utländsk påverkan.

Sakerhet · Politik · Konkurrens · 1 observation · senast 1 augusti 2026

Källor

01 **Sociala medier och valmanipulation: Hur säkrar vi höstens ...**
sweden.representation.ec.europa.eu

02 **Valet 2026**
mpf.se

03 **Så jobbar vi med valen 2026**
mcf.se

MAKROTREND

Kriskommunikation som proaktivt försvar

Företag och organisationer implementerar strukturerade kriskommunikationsstrategier specifikt utformade för att bibehålla förtroende under pågående desinformationskampanjer. Fokus ligger på att förutse narrativ och snabbt kunna bemöta missvisande information innan den får fäste.

Sakerhet | Effektivisering | Konkurrens | 1 observation · senast 1 augusti 2026

Källor

01 **Building Resilience Against Election Influence Operations**
ifes.org

02 **FIMI Defenders For Election Integrity (FDEI)**
disinfo.eu

MIKROTREND

Standardiserad incidentrapportering för valintegritet

Införande av strikta, tidskritiska rutiner för incidentrapportering vid val, där även allmänheten involveras i rapporteringskedjan. Detta skapar ett behov hos organisationer att implementera digitala system för att snabbt verifiera och agera på avvikelser i realtid för att skydda demokratiska processer.

Reglering | Digitalisering | Sakerhet | 1 observation · senast 1 augusti 2026

Källor

01 **Utveckling och nya regler i valsystemet – nyheter inför valen 2026 | Valmyndigheten**
val.se

MAKROTREND

Valet 2026 driver efterfrågan på desinformationsskydd för politisk kommunikation

Inför svenska valet 2026 varnar myndigheter och forskare för deepfakes, AI-genererad desinformation och påverkanskampanjer från främmande makt. Statsministern har kallat partiledarna till krismöte. Detta skapar en akut marknad för tjänster som övervakar, analyserar och motverkar desinformation i realtid, samt för strategisk rådgivning till partier och myndigheter om kommunikationssäkerhet.

Sakerhet | Politik | Konsumentbeteende | 3 observationer · senast 1 augusti 2026

Källor

01 **Åtgärder mot deepfakes och AI-driven desinformation (Motion 2024/25:1262 av Aida Birinxhiku (S)) | Sveriges riksdag**
riksdagen.se

02 **Varningarna inför valet: Rykten, cyberattacker och deepfakes | SVT Nyheter**
svt.se

03 **Svenska valet 2026: AI, deepfakes och väljarnas oro - Dagens Samhälle**
dagenssamhalle.se

MAKROTREND

Algoritmisk transparens och digitalt informationsflöde i valår

En ökad press på digitala plattformar och mediehus att tillhandahålla transparens kring hur politiska budskap sprids och prioriteras. Detta driver en marknad för analysverktyg som kan kvantifiera och visualisera spridningsmönster av desinformation i realtid för att möjliggöra snabbare motåtgärder.

Digitalisering | Sakerhet | Innovation | 1 observation · senast 1 augusti 2026

Källor

01 **Hur påverkar internet våra politiska ställningstaganden?**
svenskarnaochinternet.se

02 **Sociala medier och valmanipulation: Hur säkrar vi höstens riksdagsval?**
sweden.representation.ec.europa.eu

MIKROTREND

AI-baserad verifiering för redaktionell integritet

Utveckling av specialiserade verktyg för redaktioner och organisationer för att i realtid identifiera AI-genererat eller manipulerat innehåll. Detta skiftar fokus från manuell granskning till automatiserad detektering av desinformation inför valprocesser.

Ai · Innovation · Sakerhet · 1 observation · senast 1 augusti 2026

Källor

01 **Nytt projekt ska stötta redaktioner mot desinformation inför valet**
lnu.se

02 **FIMI Defenders For Election Integrity (FDEI)**
disinfo.eu

MAKROTREND

Standardisering av 'Psykologiskt Försvar' som affärsfunktion

Företag och organisationer börjar implementera strukturerade ramverk för att skydda sitt varumärke och sin verksamhet mot otillbörlig informationspåverkan, inspirerat av myndigheternas arbete med psykologiskt försvar. Detta inkluderar risk- och sårbarhetsanalyser (RSA) specifikt inriktade på desinformation.

Sakerhet | Affarsmodeller | Kvalitet | 1 observation · senast 1 augusti 2026

Källor

01 **Riskkommunikation | Myndigheten för psykologiskt försvar**
mpf.se

02 **Krisberedskap Sverige 2026: samhällsekonomisk analys | SNS - SNS**
sns.se

03 **Crisis Communication and Combating Disinformation:**
ifes.org

MAKROTREND

Opinionsledarstrategier som krisberedskap

Systematisk användning av informella ledare (inom skola, bostadsbolag, socialtjänst) som en integrerad del av kriskommunikationsstrategier. Genom att bygga relationella nätverk före krisen skapas en motståndskraftig infrastruktur som kan motverka desinformation genom betrodda lokala röster.

Hallbarhet | Effektivisering | Sakerhet | 1 observation · senast 1 augusti 2026

Källor

01 **Kriskommunikation i ett globalt samhälle**
rib.msb.se

MAKROTREND

Resiliensbaserad riskbedömning för digital infrastruktur

Skiftet från reaktivt försvar till proaktiv resiliens där organisationer stresstestar sin digitala infrastruktur mot sofistikerade påverkansoperationer. Detta inkluderar tekniska standarder för att säkerställa att digitala processer inte kan manipuleras eller ifrågasättas i sin integritet.

Sakerhet · Teknik · Infrastruktur · 1 observation · senast 1 augusti 2026

Källor

01 **Sociala medier och valmanipulation: Hur säkrar vi höstens ...**
sweden.representation.ec.europa.eu

02 **Protecting Electoral Processes in the Information Environment**
idea.int

03 **Election Integrity**
whitehouse.gov

MAKROTREND

Interoperabilitet i FIMI-försvar (Foreign Information Manipulation and Interference)

Framväxten av nätverk och gemensamma plattformar där olika aktörer (myndigheter, akademi och civilsamhälle) delar data och metoder för att motverka utländsk informationspåverkan. Detta skapar en mer enhetlig och effektiv respons mot koordinerade påverkansoperationer.

Sakerhet | Innovation | Globalisering | 1 observation · senast 1 augusti 2026

Källor

01 **Countering information manipulation - European Commission**
commission.europa.eu

02 **FIMI Defenders For Election Integrity (FDEI)**
disinfo.eu

MIKROTREND

OSINT (Open Source Intelligence) blir standardverktyg för att upptäcka informationspåverkan

Offentlig sektor och företag börjar systematiskt använda OSINT för att tidigt identifiera desinformationskampanjer. Detta skapar en efterfrågan på utbildning, verktyg och konsulttjänster inom öppen källkodsanalys specifikt inriktad på AI-genererad desinformation.

Sakerhet | Effektivisering | Digitalisering | 3 observationer · senast 1 augusti 2026

Källor

01 **Hot mot ekonomin kan börja med ett rykte: ny rapport - Handelshögskolan**
hhs.se

02 **[PDF] Sweden's AI Strategy | Government.se**
government.se

03 **Insikter & resurser om cybersäkerhet - Junglemap**
junglemap.com

OM ANALYSEN

Använd gärna analysen

Du får gärna skriva ut, dela och citera ur analysen. Använd insikterna i ert eget arbete, i presentationer och i samtal där de kan göra nytta.

DOKUMENTKÄLLA

https://trendscope.se/strategier-for-desinformationshantering-och-valintegritet

NÄR DU HÄNVISAR

Ange Trendscope som källa. I digitala sammanhang får du gärna länka tillbaka till dokumentkällan, så att läsaren kan hitta den senaste publicerade versionen och följa underlaget vidare.

KONTROLLERA VIKTIGA UPPGIFTER

Både människor och AI kan missa sammanhang, feltolka uppgifter eller återge en källa fel. Kontrollera därför originalkällan när en uppgift ska ligga till grund för beslut, publicering eller andra sammanhang där korrekthet är viktig.

AI-STÖD OCH MÄNSKLIG KURERING

Delar av källinsamlingen och bearbetningen har gjorts med AI-stöd. Urval, struktur och den publicerade analysen har granskats och kurerats redaktionellt av människor.

FÖRESLAGEN HÄNVISNING

Trendscope. “Strategier för desinformationshantering och valintegritet”. Uppdaterad 1 augusti 2026.