RAPPORT

Myndigheten för psykologiskt försvar

UPPRÄTTAD: 2026-08-31
DIARIENUMMER: MPF/2026:402
ISBN 978-91-990892-9-4

Nätverket "Holiday"

Ett exempel på hur AI används för otillbörlig informationspåverkan

Myndigheten för psykologiskt försvar

Innehåll

Myndigheten för psykologiskt försvar

VÅXNÄSGATAN 10
653 40 KARLSTAD

TEL: 010-1837000
ORG.NR: 202100-7014

REGISTRATOR@MPF.SE
WWW.MPF.SE

Sammanfattning

- Denna rapport från Myndigheten för psykologiskt försvar, MPF, belyser två aktuella företeelser som delvis hänger ihop och förstärker varandra: utvecklingen av desinformation som tjänst och framväxten av botnätverk som drivs eller förstärks med hjälp av AI.

- **Botnätverket ”Holiday”.** Rapporten beskriver ett delvis AI-drivet botnätverk med totalt cirka 1 200 konton som MPF identifierat på plattformen X. Bedömningen är att en statlig aktör köpt nätverket från ett företag i Östasien och att nätverket under 2025 och 2026 använts för otillbörlig informationspåverkan mot Sverige och flera andra länder. Botnätverket, som av MPF fått arbetsnamnet ”Holiday”, har totalt gjort över 50 000 inlägg, kommentarer och delningar, merparten med fokus på dagsaktuella politiska förslag eller utspel som diskuterats flitigt på plattformen. Nätverket har agerat tydligt polariserande. Medan en del konton i nätverket uttryckt mycket positiva åsikter har andra konton varit starkt negativa i samma fråga. Nätverket har också interagerat med vanliga, riktiga användare på X.

- **Myndighetssamverkan.** Flera myndigheter har bidragit till att botnätverket upptäckts och kunnat stängas ned. De första kontona upptäcktes av Riksbanken, efter att de genomfört en MPF-ledd övning i syfte att proaktivt stärka sin förmåga att upptäcka och hantera otillbörlig informationspåverkan. MPF kunde senare konstatera att botkontona var en del av ett större nätverk som över tid växte och blev mer sofistikerat. Genom samverkan mellan MPF och Post- och Telestyrelsen, PTS, uppmärksammades X på nätverket, vilket resulterade i att samtliga konton stängdes av från plattformen.

- **Otillbörlig informationspåverkan med hjälp av AI.** MPF:s syfte med att beskriva botnätverket i en öppen rapport är att belysa och konkretisera hur AI kan användas för otillbörlig informationspåverkan. Medvetenhet om hur hotbilden från otillbörlig informationspåverkan ser ut är en viktig förutsättning för motståndskraft.

- **Råd till privatpersoner och verksamheter.** I rapporten finns ett antal konkreta råd och rekommendationer, både till privatpersoner och till verksamheter. Som privatperson är det bra att vara medveten om att det finns statliga aktörer och andra utländska hotaktörer som med hjälp av AI försöker manipulera informationsmiljön. Syftet kan till exempel vara att polarisera, trissa upp tonläget och skapa ökad oro kring en viss fråga. Det är klokt att vara vaksam på innehåll som väcker starka känslor, alltid kontrollera källan och försöka bekräfta information innan den delas vidare. För offentliga aktörer och andra verksamheter är det bra att stärka sin förmåga att upptäcka botnätverk och annan misstänkt otillbörlig informationspåverkan samt ha beredskap för att kunna hantera händelser.

Genom ökad förmåga att upptäcka, hantera och stå emot otillbörlig informationspåverkan stärker vi tillsammans Sveriges psykologiska försvar.

Om Myndigheten för psykologiskt försvar

Sverige är ett öppet och demokratiskt land. Det gör oss starka, men vi är också en potentiell måltavla för yttre hotaktörer som vill skada oss genom desinformation, vilseledning och andra former av otillbörlig informationspåverkan. Myndigheten för psykologiskt försvar, MPF, arbetar med att identifiera, analysera och motverka dessa försök till påverkan från främmande makt och andra utländska hotaktörer.

För att stärka hela Sveriges motståndskraft utbildar och övar vi myndigheter, andra samhällsaktörer och ytterst befolkningen om otillbörlig informationspåverkan från utländska hotaktörer. Det psykologiska försvaret bygger vi tillsammans.

Inledning

De senaste årens snabba AI-utveckling har i grunden förändrat förutsättningarna för utländska hotaktörer med avsikt att försöka manipulera informationsmiljön. AI används för att producera eller manipulera till exempel bilder och videos, men det har också med AI:s hjälp blivit väsentligt enklare att sprida stora mängder information eller målgruppsanpassa påverkansförsök. Teknikutvecklingen har även skapat nya möjligheter för den som vill dölja vem som är den egentliga avsändaren bakom information.

Dolda påverkansstrukturer kan till exempel vara nätverk av falska nyhetssidor som sprider stora mängder manipulerade eller uppdiktade nyheter. Dessa kan i sin tur förstärkas av botnätverk som drivs med hjälp av AI, eller samordnade nätverk av konton som använder falska eller vilseledande identiteter. Sammantaget brukar den här typen av manipulation av informationsmiljön benämnas koordinerat icke-autentiskt beteende (ofta förkortat KIB eller på engelska CIB, för *coordinated inauthentic behaviour*). Det är viktigt att understryka att koordinerat icke-autentiskt beteende inte handlar om huruvida information är sann eller falsk, det är det manipulativa beteendet som är kärnan.

AI-utvecklingen utnyttjas av utländska hotaktörer, vars syfte ofta är att så misstro eller split och påverka våra uppfattningar, beteenden eller beslut. Detta kan medföra en rad demokratiska risker, så som minskat förtroende för offentliga institutioner, ökade motsättningar, polarisering och valpåverkan.

MPF vill med den här rapporten belysa, konkretisera och öka medvetenheten om otillbörlig informationspåverkan med hjälp av AI. Inledningsvis i rapporten beskrivs en annan företeelse som delvis hänger ihop med och förstärker nyttjandet av AI: utvecklingen av desinformation som tjänst. Sist i rapporten finns ett avsnitt med råd och rekommendationer, både till privatpersoner och till offentliga verksamheter och andra organisationer.

Utvecklingen av desinformation som tjänst

Fenomenet desinformation som tjänst (på engelska används bland annat begreppen *disinformation as a service* eller *disinformation for hire*) har genomgått en betydande utveckling de senast 15 åren. Det som initialt utgjordes av så kallade trollfarmar, som krävde manuell handpåläggning av riktiga personer, har över tid utvecklats till en global industri som inkluderar statskopplade eller privata aktörer så som konsulter, PR- och marknadsföringsfirmor.

Utvecklingen kan förenklat beskrivas ha skett i tre olika faser. Under den tidiga fasen (ca 2010 – 2018) utvecklades desinformation från mer isolerade propagandaförsök till att bli en återkommande påverkansmetod för främmande makt. Falska personas, koordinerade inlägg, botar och riktad reklam användes för att manipulera diskursen online. Statliga aktörer, som tidigare velat ha fullständig kontroll på kampanjerna, började nu lägga ut stora delar av utförandet på privata aktörer med koppling till staten.

I den andra fasen (ca 2019 – 2024) blev det allt vanligare att privata företag började erbjuda och sälja påverkansoperationer. Manipulation var inte längre något som främst auktoritära stater utförde. Kommersiella aktörer hjälpte också till att sudda ut gränsen mellan marknadsföring och mer dolda propagandaförsök. Desinformation blev en egen serviceindustri med politiska konsulter som erbjöd dold manipulation, betalda influerare som spred koordinerade politiska narrativ, engagemangsfarmer, falska nätverk med influerare och koordinerade hashtag-kampanjer. Flera valpåverkansförsök med hjälp av dessa metoder noterades.

Den tredje fasen, som vi fortfarande befinner oss i, karaktäriseras av hur generativ AI i grunden förändrat förutsättningarna att bedriva otillbörlig informationspåverkan. Påverkanskampanjer som tidigare varit relativt arbetsintensiva är nu kostnadseffektiva, skalbara och allt mer automatiserade. De tidigare så kallade trollfarmerna har i hög grad ersatts av allt mer AI-drivna botnätverk, med konsekvensen att en informationskampanj kan drivas från en enskild dator. AI kan användas för att driva tusentals falska sociala mediekonton och generera flerspråkigt innehåll för specifika målgrupper i realtid. Med hjälp av AI kan också lokala och kulturella referenser vävas in som gör det enklare att smälta in i den inhemska informationsmiljön.

Syftet med informationspåverkanskampanjer är ofta att på olika sätt manipulera den fria opinionsbildningen genom att artificiellt undertrycka eller förstärka vissa åsikter eller visst innehåll på sociala medier. När kampanjer lejs ut på privata företag ger det statliga aktörer ökad strategisk räckvidd och förnekbarhet. Samtidigt informationstvättas desinformationen, det vill säga avsändaren blir en annan och det blir svårt för gemene man att veta dess ursprung. Information, som härstammar från en utländsk hotaktör, kan exempelvis mot betalning delas av en influerare med stor följarskara. När information plockas upp och sprids vidare, ofta med en kombination av organisk spridning och förstärkning från till exempel botnätverk, är informationens ursprung svår att identifiera.

Att köpa olika former av engagemang på sociala medier är förhållandevis enkelt och billigt. Tjänsterna kan nyttjas av allt från influerare eller företag som vill ha större genomslag, till kriminella aktörer som begår bedrägerier eller främmande makts påverkanskampanjer. Det finns hemsidor där man kan beställa allt från fullskaliga påverkanskampanjer till enskilda delar som likes, följare, visningar, delningar, kommentarer, verifierade konton, gamla konton och äkta konton – allt för att öka spridningen på visst innehåll och framstå som en trovärdig källa. Konton som drivs med hjälp av AI kan skapa stora mängder kommentarer och inlägg, simulera olika politiska åsikter samt skapa en illusion av folkligt stöd. AI hjälper också till att anpassa innehållet genom att analysera trender, nyheter och reaktioner i realtid och justera budskapen beroende på användarnas respons.

MPF har analyserat utbudet på flera tjänster som säljer olika former av engagemang på sociala medier. Som ett exempel på hur marknaden ser ut finns i tabellen nedan ungefärliga prisintervall hösten 2026 för köp av engagemang på sociala medier (X/Twitter, Instagram,

Facebook, TikTok med flera). Samtliga priser i tabellen avser köp av 1 000 stycken, till exempel likes, följare eller kommentarer. Variationen i pris beror bland annat på vilken typ av konton som avses (bot- eller ”riktiga”/aktiva konton) samt till viss del vilken social medieplattform det gäller.

Typ	Lägsta pris/1 000 st	Högsta pris/1 000 st	Kommentar
Gilla-markeringar	0,20 kr	250 kr	Priset varierar beroende på om gilla-markeringen kommer från rena botkonton eller "riktiga"/aktiva konton.
Följare	0,50 kr	600 kr	Botkonton är billigast, geo-riktade (till exempel svenska konton) och "riktiga" följare kostar mer.
Kommentarer	10 kr	3 000 kr	Priset varierar beroende på typ av kommentarer: generiska, negativa och positiva, samt mänskliga/skräddarsydda.
Delningar	3 kr	2 000 kr	Priset varierar kraftigt beroende på köp av delning eller köp av delning av inlägg med kommentar.
Visningar	0,20 kr	150 kr	Priset varierar främst beroende på vilken plattform visningarna ska ske på.
Omnämnande	40 kr	180 kr	Priset varierar beroende på om kontona som omnämner det önskade kontot även ska vara följare eller ha reagerat på inlägg från kontot.

AI-drivna botnätverk – fallet ”Holiday”

För att konkretisera hur desinformation som tjänst kan ta sig uttryck beskrivs här ett botnätverk som MPF identifierat. Nätverket har varit aktivt 2025 – 2026 och drivit otillbörlig informationspåverkan mot Sverige och flera andra länder. Totalt genomförde nätverket över 50 000 aktiviteter på X i form av enskilda inlägg, svar och delningar av andras innehåll.

MPF genomför regelbundet övnings- och utbildningsinsatser för myndigheter och andra aktörer för att bidra till ökad kunskap om psykologiskt försvar. Ett viktigt syfte med sådana övningar är att stärka aktörers förmåga att upptäcka och hantera otillbörlig informationspåverkan. Efter att MPF genomfört en sådan övning hos Riksbanken, kontaktade de MPF då de identifierat icke-autentiskt beteende från ett antal konton i myndighetens sociala medieflöde. MPF undersökte informationen och kunde konstatera att kontona ingick i ett större botnätverk av icke-autentiska konton som polariserade debattklimatet på plattformen X. Nätverket fick av MPF arbetsnamnet ”Holiday”, då nätverket initialt postade inlägg om semesterplaner.

Nätverket identifieras

När MPF började analysera informationen visade det sig att ett nätverk av cirka 200 botkonton på X skapats under våren 2025. Nätverket förenades av en uppsättning gemensamma attribut, beteendemönster och tekniska egenskaper. Nätverkets konton var fördelade mellan flera olika språkgrupper, varav svenska var en. Ett 60-tal konton utgav sig för att vara svenska X-användare och använde AI-genererade profilbilder, svenskklingande namn och skrev på god

svenska. Genom manipulering av platsdata såg alla konton ut att vara uppkopplade från Sverige. Samtliga konton var över 10 år gamla men hade under våren 2025 bytt användarnamn och raderat spår av tidigare aktivitet.

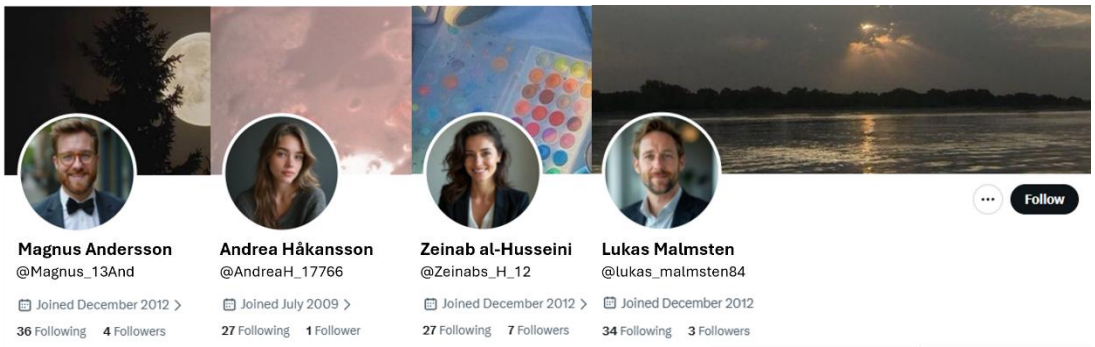

Bild 1: Exempel på hur kontona i den svenska delen av nätverket såg ut. Nätverkets konton karaktäriserades av generiska, AI-genererade bilder, låga följarantal och liknande skapandedatum.

Fas 1 – polarisering enligt tydliga teman

Under våren 2025 agerade nätverket polariserande genom att ge uttryck för motstridiga åsikter i en mängd olika frågor. Medan en del av nätverket skrev mycket positiva kommentarer i en viss fråga postade andra konton i nätverket mycket negativa inlägg i samma fråga. Nätverkets aktivitet var särskilt centrerad kring nya politiska förslag eller utspel från regeringsföreträdare och oppositionspartier.

Nätverkets konton hade tydliga och konsekventa intressen – de var antingen för eller emot regeringen och intresserade sig för specifika sakfrågor som invandring, ekonomi eller klimat och hållbarhet. Samtidigt skrev nätverket även om andra vardagliga ämnen som fotbollsmatcher i allsvenskan eller längtan efter stundande semester, troligtvis i syfte att skapa en mer ”mänsklig” digital persona.

Under slutet av 2025 inaktiverades nätverket tillfälligt. Det finns flera möjliga förklaringar till avbrottet – det kan till exempel ha varit en planerad del av en längre utvecklingsprocess, ha föregåtts av förändrade instruktioner från beställaren eller vara en åtgärd för att försöka undgå upptäckt.

Bild 2: Exempel på aktivitet under fas 1. Vid givna tillfällen polariserar nätverkets konton debatten kring särskilda frågor. Nätverket använder ”hashtags” för ökad spridning.

Fas 2 – ett större och mer autonomt nätverk

När nätverket efter några månader åter aktiverades hade det utvecklats i flera avseenden. Nätverket hade vuxit till totalt cirka 1 200 konton, var aktivt dygnet runt och interagerade direkt med autentiska konton, inklusive större svenska konton på X. Kontona använde nu också sarkasm, humor och hade ett mer retoriskt förfinat språkbruk än under fas 1. Nätverkets konton var också tydligt fokuserade på att polarisera i ämnen som för stunden ”trendade” bland svenska X-användare.

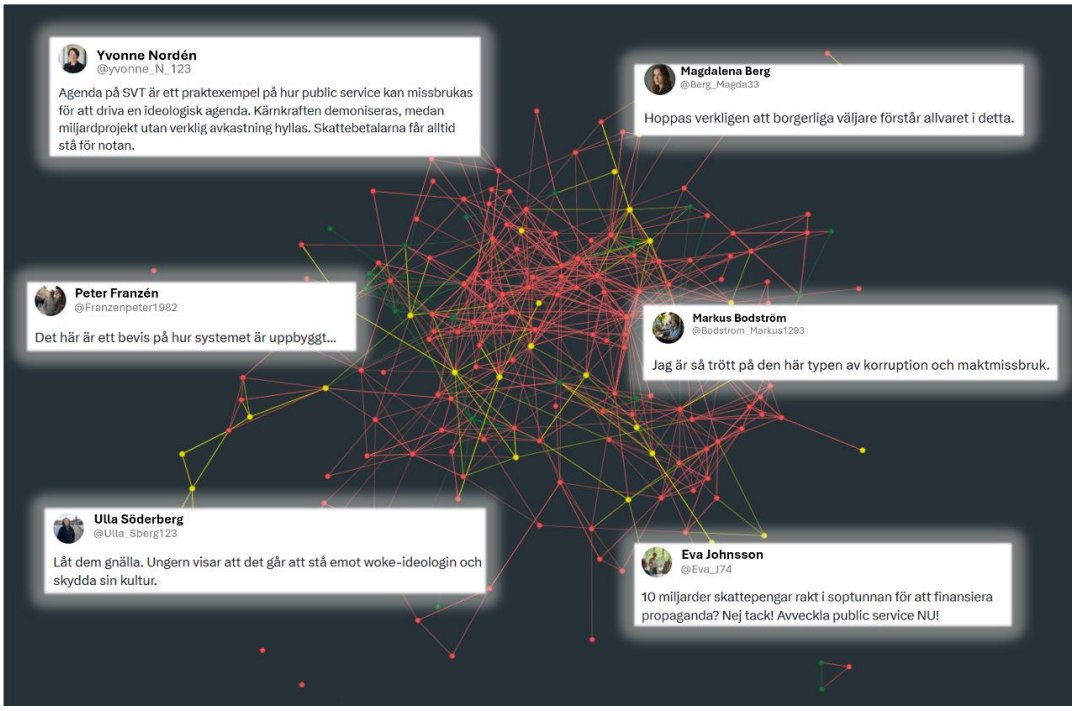

Bild 3: Sentimentkarta från en dag under våren 2026 som visar nätverkets polariserande effekt i olika diskussioner inom den svenska informationsmiljön på X. Varje markering motsvarar ett X-inlägg och färgen beskriver inläggets ”tonläge”. Röda inlägg motsvarar ”negativa” inlägg, gröna ”positiva” och gula ”neutrala”. Infogade inlägg är exempel på nätverkets aktivitet.

Med nya och förfinade funktioner lämnade nätverket nu ett större avtryck i den svenska informationsmiljön: inläggen fick fler visningar och gilla-markeringar, men genererade även svar från riktiga svenska X-användare. Förutom att polarisera i de mest omdiskuterade samtalsämnena på X deltog nätverket även i drev mot svenska politiker och offentliga personer, myndigheter, företag eller enskilda mediehus.

En statlig aktör och en leverantör i Östasien

Kommersialiseringen av desinformation, som beskrevs inledningsvis, har inneburit att en påverkansoperation kan läggas ut på entreprenadrån beställaren till en extern aktör. MPF kan konstatera att populationer av icke-autentiska konton ofta går att härleda till leverantörer i Asien eller Afrika även om samma tjänster också tillhandahålls av aktörer i bl.a. Europa. När det gäller botnätverket som vi här kallar ”Holiday-nätverket” finns tydliga indikationer på att det skapats av en leverantör i Östasien. MPF har även belägg för att det är en statlig aktör som

beställt och ligger bakom nätverket, men någon definitiv teknisk attribuering har inte gjorts. Generellt kan dock konstateras att det finns flera statliga aktörer som återkommande agerar på motsvarande sätt i informationsmiljön.

Den aktuella östasiatiska leverantören erbjuder en portfölj av helt eller delvis illegala tjänster inom bland annat digitala intrång, kartläggning och publicering av personlig information i syfte att skrämma eller hota (så kallad *doxxing*) och koordinerade smutskastningskampanjer. Leverantören riktar sig till en global kundkrets och annonserar sitt utbud av tjänster och tar emot beställningar via olika kanaler på Telegram. Det går att köpa färdiga populationer om hundra- eller tusentals icke-autentiska sociala mediekonton. Leverantören erbjuder sig även att sköta driften av botnätverk enligt kundens önskemål. Prissättningen beror på hur sofistikerat och stort nätverket är och behov av lokal handpåläggning. Exempelvis ökar priset på ett TikTok-konto om kontona i nätverket är flera år gamla, ID-verifierade och har många följare.

Det är inte ovanligt att icke-autentiska konton återanvänds från en kampanj till en annan. Exempelvis kunde MPF konstatera att konton som ingick i Holiday-nätverket tidigare använts i kampanjer mot andra målgrupper, bland annat i USA, Kina och Taiwan. Nätverkets konton hade då andra profilbilder och namn och skrev på andra språk. Kampanjerna hade sannolikt skapats och sålts av samma östasiatiska leverantör, men beställts av andra aktörer.

Nätverket stängs ned

Sociala medier-företag och plattformar har ett viktigt ansvar att motverka desinformation. EU-förordningen om digitala tjänster (Digital Services Act, DSA), har skärpt kraven på stora digitala plattformar att driva ett systematiskt arbete med att identifiera, bedöma och begränsa systemrisker, till exempel risker som kan uppstå genom samordnade desinformationskampanjer. I Sverige är det Post och Telestyrelsen, PTS, som är samordnare för digitala tjänster och har uppdraget att bland annat följa upp att reglerna i DSA följs i Sverige.

Med anledning av det identifierade nätverket har MPF samverkat med PTS och uppmärksammat X på nätverket. X bedömde att kontona bröt mot plattformens egna riktlinjer om koordinerat icke-autentiskt beteende. Detta ledde till att samtliga konton i nätverket under sommaren 2026 stängdes ned av X.

Råd och rekommendationer

Att vara medveten om hur hotet när det gäller otillbörlig informationspåverkan kan se ut är centralt för att bygga motståndskraft. Denna rapport belyser två aktuella företeelser som delvis hänger ihop och förstärker varandra: utvecklingen av desinformation som tjänst och framväxten av botnätverk som drivs med hjälp av AI.

Nedan listas ett antal konkreta råd och rekommendationer, både till privatpersoner och till verksamheter.

Läs gärna mer på myndighetens webbplats www.mpf.se. Där finns både råd för privatpersoner och Förmågeportalen där MPF samlat stöd och kunskapsmaterial för offentliga aktörer och andra verksamheter.

Råd till privatpersoner

- **Se upp.** Det är viktigt att vara medveten om att gilla-markeringar, visningar, kommentarer och följare enkelt, snabbt och billigt kan köpas, och att det finns utländska hotaktörer som utnyttjar detta för att manipulera informationsmiljön. Var vaksam på information, bilder eller annat som upprör, skapar starka känslor eller skrämmer. Botnätverk som drivs med hjälp av AI kan försöka bidra till att tonläget trissas upp kring en viss fråga, att en viss åsikt framstår som mer utbredd än vad den egentligen är eller att polarisering framstår som väsentligt större än vad som är fallet.
- **Tänk efter.** Undvik att bli en del i spridningen av desinformation, vilseledande information och propaganda. Det är klokt att tänka efter innan du delar vidare information.
- **Kolla källan.** Kontrollera källan. Botkonton som drivs med hjälp av AI är ibland svåra att identifiera, men det kan finnas varningssignaler. Var uppmärksam på till exempel uppenbart AI-genererade profilbilder med få följare, språkanvändning med tecken på maskinöversättning och generiska intetsägande profiler med till exempel nummer och slumpade bokstäver i profilnamnet.
- **Sök bekräftad information.** Sök information hos myndigheter. Använd gärna olika typer av kanaler för att söka information. Komplettera sociala medier med TV, traditionella medier, poddar och andra informationskällor. Använd flera olika sociala medier.

Om du upptäcker olagligt innehåll på sociala medier kan du anmäla det till den aktuella plattformen. De är skyldiga att ha tjänster där anmälningar kan göras. Vid misstänkt brottslighet som till exempel bedrägerier: polisanmäl.

Råd till offentliga aktörer och andra verksamheter

Offentliga aktörer och andra verksamheter är ofta de som kan upptäcka botkonton som drivs med hjälp av AI och andra former av misstänkt otillbörlig informationspåverkan från utländska hotaktörer. Nedan ges därför ett antal råd till offentliga aktörer och andra verksamheter.

1. Upptäck

Stärk er förmåga att upptäcka botnätverk och annan misstänkt otillbörlig informationspåverkan från utländska hotaktörer.

- **Normalbild**. Skapa en förståelse för normalbilden när det gäller aktivitet i era sociala mediekanaler/flöden, till exempel antal följare/gilla-markeringar/kommentarer/omnämningar per inlägg som kan anses normalt under en given tidsperiod.
- **Avvikelser**. En löpande bevakning gör det enklare att upptäcka avvikelser som till exempel en mycket stor ökning av antalet följare, kommentarer eller omnämnanden som inte kan förklaras av andra faktorer.
- **Misstänkt koordinerad icke-autentisk aktivitet.** Tecken på botnätverk eller andra former av koordinerat icke-autentiskt beteende kan vara till exempel stora mängder konton som använder snarlika namn profilbilder eller formuleringar om samma saker vid samma tidpunkt, uppenbart AI-genererade profilbilder, språkanvändning med tecken på maskinöversättning eller generiska intetsägande profiler med t.ex. nummer och slumpade bokstäver i profilnamnet.

2. Hantera

Enstaka botkonton förekommer i nästan alla sociala medie-flöden. Om ni upptäcker större mängder misstänkta botkonton eller andra former av koordinerat icke-autentiskt beteende i era flöden kan ni behöva agera mer samlat.

- **Ta ställning och bygg kunskap i förväg.** Det underlättar att ha en policy eller riktlinje där ni i förväg tagit ställning till hur ni hanterar icke-autentiskt beteende på era sociala medier. De flesta större sociala medieplattformar har egna regler för koordinerat icke-autentiskt beteende. Det kan vara bra att ha kunskap om regelverken på de plattformar där ni själva agerar.
- **Överväg att anmäla.** Om inlägg och kommentarer i era sociala mediekanaler bryter mot plattformarnas regler kan en första åtgärd vara att rapportera detta till plattformen. Om ni bedömer att det handlar om misstänkt brottslighet: polisanmäl. Om ni misstänker att en utländsk hotaktör ligger bakom kan ni kontakta MPF för stöd.

Ett starkt psykologiskt försvar skapas tillsammans.