hi5h five

01

OM HIGHFIVE

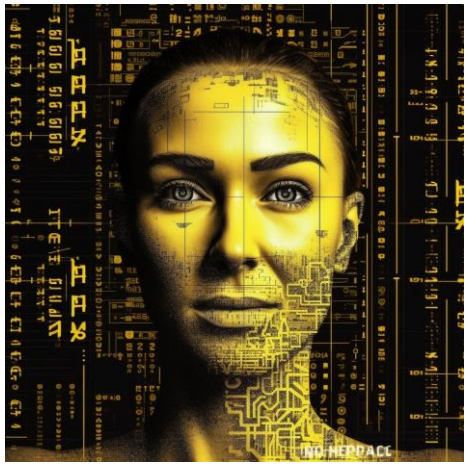
HIGHFIVE = INNOVATIONSARENA

Inkubator Studentinkubator Projektarena Offentlig sektor


Akademi
Näringsliv
Offentlig sektor
Samhället

FOKUSOMRÅDEN

Diaitaliserina & datadriven innovation



Människocentrerad AI

Cybersäkerhet

Hållbarhet

AI Act i Halland – Innovation & stöd för SMF

Syftet med projektet är att utveckla kompetens, metoder och arbetssätt som hjälper innovationsstödjande aktörer samt SMF i Region Halland att effektivt anpassa sig till den nya AI-lagstiftningen (AI Act). Vi strävar efter att säkerställa att företag kan förstå och uppfylla lagens krav utan att deras innovationskraft och konkurrenskraft minskar.

- **Kartläggning**
- **Kompetensutvecklingsinsatser & workshops**
- **Guider & verktyg**
- **Kunskapsdelning**
- **Tekniketiskt center**

Läs mer och ta kontakt här: AI Act | HighFive Innovationsarena

CYBERSÄKERHET

Studenter i Halmstad rekryteras för att hacka halländska företag | SVT Nyheter

Dagens industri START BÖRS MARKNADSNYTT BEVAKNINGAR LEDARE DI TV

Innehåll från Intility

ya NIS2-direktivet syftar till att motverka
gen av cyberattacker mot europeiska företag
täller omfattande krav på IT-säkerhet.
förväntas omfatta 10 000 svenska
amheter, men kan potentiellt vara tillämpligt för
nga som 20 000.

EXPRESSEN

Attack mot Skatteverket – mitt i deklarationen

Publicerad 18 mar 2025 kl 12.23
Uppdaterad kl 19.54

Mitt i deklarationen slog marodörerna till.

Överbelastningsattacker har gjort det svårt att i omgångar komma in på Skatteverket sedan 07 imorse.

– Det är en attack från utlandet, säger it-direktören Peder Sjölander.

Dataintrång satte företag i konkurs

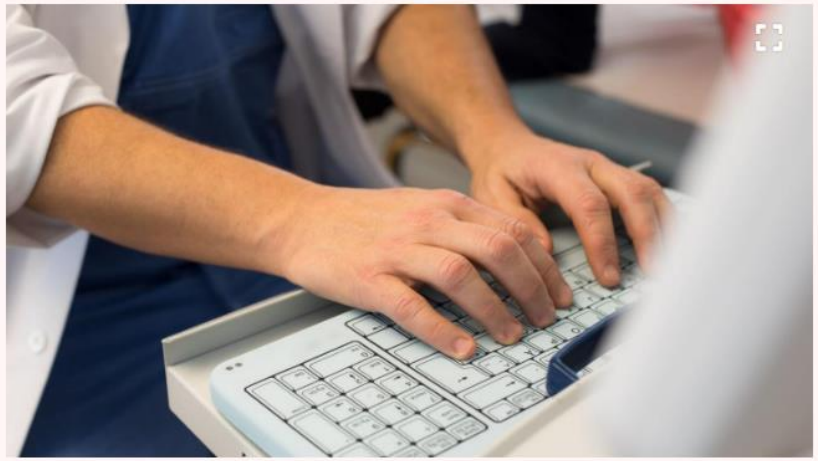


Bild: Mostphotos

Flera utpressningsförsök och dataintrång satte det finska psykoterapicentret Vastaamo i konkurs, skriver Aktuell Säkerhet

En massiv dataläcka a
upptäcktes i oktober 2
diskussionsforum på i
pressmeddelande från

– Fallet Vastaamo är e
illa vid ett dataintrång.
vad är det värsta som
tiotusentals patientjou

Kostnaderna, både i ar
fortsätta bedriva verks

Tre månader villkorligt för Vastaamo-vd efter dataintrång

Psykoterapicentret Vastaamos tidigare vd döms till tre månaders villkorligt fängelse för dataskyddsbrott.

BROTT, LAG OCH RÄTT

Ville Tapio, grundare och ex-vd för psykoterapicentret Vastaamo har nekat till brott. Helsingfors tingsrätt fäller honom för dataskyddsbrott. Bristande skydd och anonymisering gjorde att patientuppgifter kunde stjälas och utnyttjas. VESA MOILANEN/LEHTIKUVA

AFTONBLADET MÅNDAG 26 FEBRUARI 2024
Dagens namn: Torgny, Torkel

Oron inifrån hackade it-jätten: ”Kommer ta månader”

Anställd berättar: ”Mörkertalet är enormt”

Ebba Thornéus

Publicerad 2024-02-08

+ Följ Mejla Dela Spara

Hackerattacken mot det privata it-bolaget slog mot myndigheter, regioner och flera stora företag.

Efter två veckor av att släcka bränder, vittnar nu en anställd om oron inifrån bolaget som drabbades av angreppet.

– Mörkertalet är enormt, säger en Tietoevry-anställd till Aftonbladet.

Ett företag som prioriterar säkerhet minskar risken för dataintrång och cyberattacker, vilket kan leda till förlust av känslig information och/eller ekonomiska skador.
”Kunna jobba”

Skydda verksamheten


EXPRESSEN

Attack mot Skatteverket – mitt i deklarationen

Publicerad 18 mar 2025 kl 12.23
Uppdaterad kl 19.54

Mitt i deklarationen slog marodörerna till.
Överbelastningsattacker har gjort det svårt att i omgångar komma in på Skatteverket sedan 07 imorse.
– Det är en attack från utlandet, säger it-direktören Peder Sjölander.


MÅNDAG 26 FEBRUARI 2024
Dagens namn: Torgny, Torkel

…nifrån hackade it- …”Kommer ta …ler”

…r: ”Mörkertalet är enormt”

Publicerad 2024-02-06

+ Följ Mejla Dela Spara

Hackerattacken mot det privata it-bolaget slog mot myndigheter, regioner och flera stora företag.
Efter två veckor av att släcka bränder, vittnar nu en anställd om oron inifrån bolaget som drabbades av angreppet.
– Mörkertalet är enormt, säger en Tietoevry-anställd till Aftonbladet.


Dagens industri START BÖRS MARKNADSNYTT BEVAKNINGAR LEDARE DI TV

Innehåll från Intility

Det nya NIS2-direktivet syftar till att motverka ökningen av cyberattacker mot europeiska företag och ställer omfattande krav på IT-säkerhet. NIS2 förväntas omfatta 10 000 svenska verksamheter, men kan potentiellt vara tillämpligt för så många som 20 000.

Efterleva lagar/regler

Bevara företagets renommé

Ett företag som prioriterar säkerhet minskar risken för förtroendeförlust från kunder och partners.
”Få/behålla kunder”

Trenden går mot mer formella krav på säkerhet. Bolag påverkas både direkt men kanske framförallt indirekt i egenskap av leverantör till kunder som omfattas av regleringar.
”Få jobba”


Dataintrång satte företag i konkurs

Bild: Mostphotos

Flera utpressningsförsök och dataintrång satte det fi… psykoterapicentret Vastaamo i konkurs, skriver Aktu…

En massiv datastöld av patientdata från det finska psykoterapicentret … upptäcktes i oktober 2020. Då laddades nära 32 000 finländares pers… diskussionsforum på internet, skriver Aktuell Säkerhet och hänvisar t… pressmeddelande från företaget.

– Fallet Vastaamo är ett exempel på worst case-scenario. Det är ova… illa vid ett dataintrång. Men, samtidigt behöver företag med känsliga … vad är det värsta som kan hända? Det är inte ironiskt att föreställa s… tiotusentals patientjournaler läcker ut, säger John Daniels, vd på We…

Kostnaderna, både i anseende och pengar efter intrånget har nu gjort det omöjligt att fortsätta bedriva verksamheten, enligt företaget.

Tre månader villkorligt för Vastaamo-vd efter dataintrång

Psykoterapicentret Vastaamos tidigare vd döms till tre månaders villkorligt fängelse för dataskyddsbrott.

hi5h five

KONKURRENSKRAFT

Skydda verksamheten

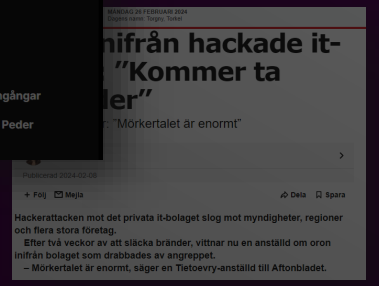
Ett företag som prioriterar säkerhet minskar risken för dataintrång och cyberattacker, vilket kan leda till förlust av känslig information och/eller ekonomiska skador.
"Kunna jobba"


EXPRESSEN

Attack mot Skatteverket – mitt i deklarationen

Publicerad 18 mar 2025 kl 12.23
Uppdaterad kl 19.54

Mitt i deklarationen slog marodörerna till.
Överbelastningsattacker har gjort det svårt att i omgångar komma in på Skatteverket sedan 07 imorse.
– Det är en attack från utlandet, säger it-direktören Peder Sjölander.


…nifrån hackade it- … "Kommer ta …ler"
… "Mörkertalet är enorm"
Publicerad 2024-02-06
Följ Mejla Dela Spara
Hackerattacken mot det privata it-bolaget slog mot myndigheter, regioner och flera stora företag.
Efter två veckor av att släcka bränder, vittnar nu en anställd om oron inifrån bolaget som drabbades av angreppet.
– Mörkertalet är enormt, säger en Tietoevry-anställd till Aftonbladet.

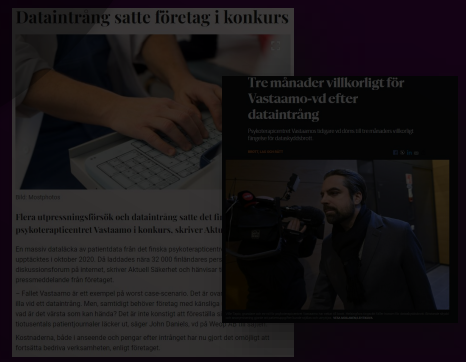

Industri
Det nya NIS2-direktivet syftar till att motverka … ökningen av cyberattacker mot europeiska … och ställer omfattande krav på IT-säkerhet. NIS2 förväntas omfatta 10 000 svenska verksamheter, men kan potentiellt vara tillämp… för så många som 20 000.

Efterleva lagar/regler

Trenden går mot mer formella krav på säkerhet. Bolag påverkas både direkt men kanske framförallt indirekt i egenskap av leverantör till kunder som omfattas av regleringar.
"Få jobba"

Bevara företagets renommé

Ett företag som prioriterar säkerhet minskar risken för förtroendeförlust från kunder och partners.
"Få/behålla kunder"


Dataintrång satte företag i konkurs

Tre månader villkorligt för Vastaamo-vd efter dataintrång

hi5h five

PROJEKTINFORMATION

Säker Digitalisering Halland 3.0

Utlysning: Stärk små och medelstora företag i Västsverige (Eruf via Tillväxtverket)

Budget: 6 500 000

Projektperiod: 2025 – 2027

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

Region Halland
BÄSTA LIVSPLATSEN

PROJEKTINFORMATION

Säker Digitalisering Halland 3.0

Projektet syftar till att skapa ett mer konkurrenskraftigt näringsliv i Halland genom stötta halländska bolags arbete med säkerhet. Projektet bygger på lärdomar från att ha skapat och genomdrivit liknande projekt, genom att ha ett holistiskt synsätt på säkerhet men även genom att undersöka helt nya möjligheter av stöd till bolag för att öka innovationskapaciteten inom området säkerhet i Halland.

Projektet består av flera arbetspaket såsom företagsspecifika insatser för att skapa nulägesanalyser kring säkerhet och handlingsplaner för förflyttning, faktiska tester av den digitala och fysiska säkerheten, hackathon för samverkan mellan näringsliv, extern expertis och akademi, insatser för att utveckla den regionala spetskompetensen kring Cybersäkerhet och AI, nätverksträffar samt större event. Aktiviteter som tillsammans kommer göra en stor inverkan på den övergripande medvetenheten kring och faktiska nivån på säkerheten hos det halländska näringslivet.

PROJEKTINFORMATION

Säker Digitalisering Halland 3.0

Mål:

- skapa en mätbar förflyttning gällande säkerhetsnivå,
- öppnare samtalsklimat kring säkerhet,
- nätverk kring säkerhet som konkurrenskraft,
- ökad beställarkunskap inom säkerhet,
- säkerhetsarbete förankrat i och drivet av bolagets högsta ledning,
- insikter om ev. digitala och fysiska säkerhetsbrister för att identifiera och åtgärda svaga punkter,
- ökat entreprenörskap hos framför allt studenter i Halland för att möta näringslivets behov och samtidigt behålla kompetens i regionen,
- ökad innovationsgrad inom cybersäkerhet med stöd av regionens spetskompetens inom AI med potentiella effekter i form av nya produkter/tjänster, nya arbetssätt och/eller nya bolag.

Kompetenshöjande och ekosystemsfrämjande aktiviteter

NÄTVERK & EVENT

Under perioden kommer vi utveckla nätverk för säkerhet och komplettera med tre större kompetenshöjande event. Att ha både årliga stora kompetenshöjande evenemang och mindre, specifika och kontinuerliga nätverksträffar om informationssäkerhet, IT-säkerhet och cybersäkerhet kan dessa komplettera varandra på flera sätt och ge ett mer komplett och hållbart tillvägagångssätt för att hantera säkerhetsutmaningar.

FÖRETAGSSPECIFIKA INSATSER

SÄKERHETSMÅNADEN

Säkerhetsmånaden är en unik process där man under en fyraveckorsperiod får verktyg och individanpassad kvalificerad rådgivning. Målet är att göra säkerhet till en integrerad och regelbunden del av sin verksamhets framtida utveckling.

Deltagande bolag: 50

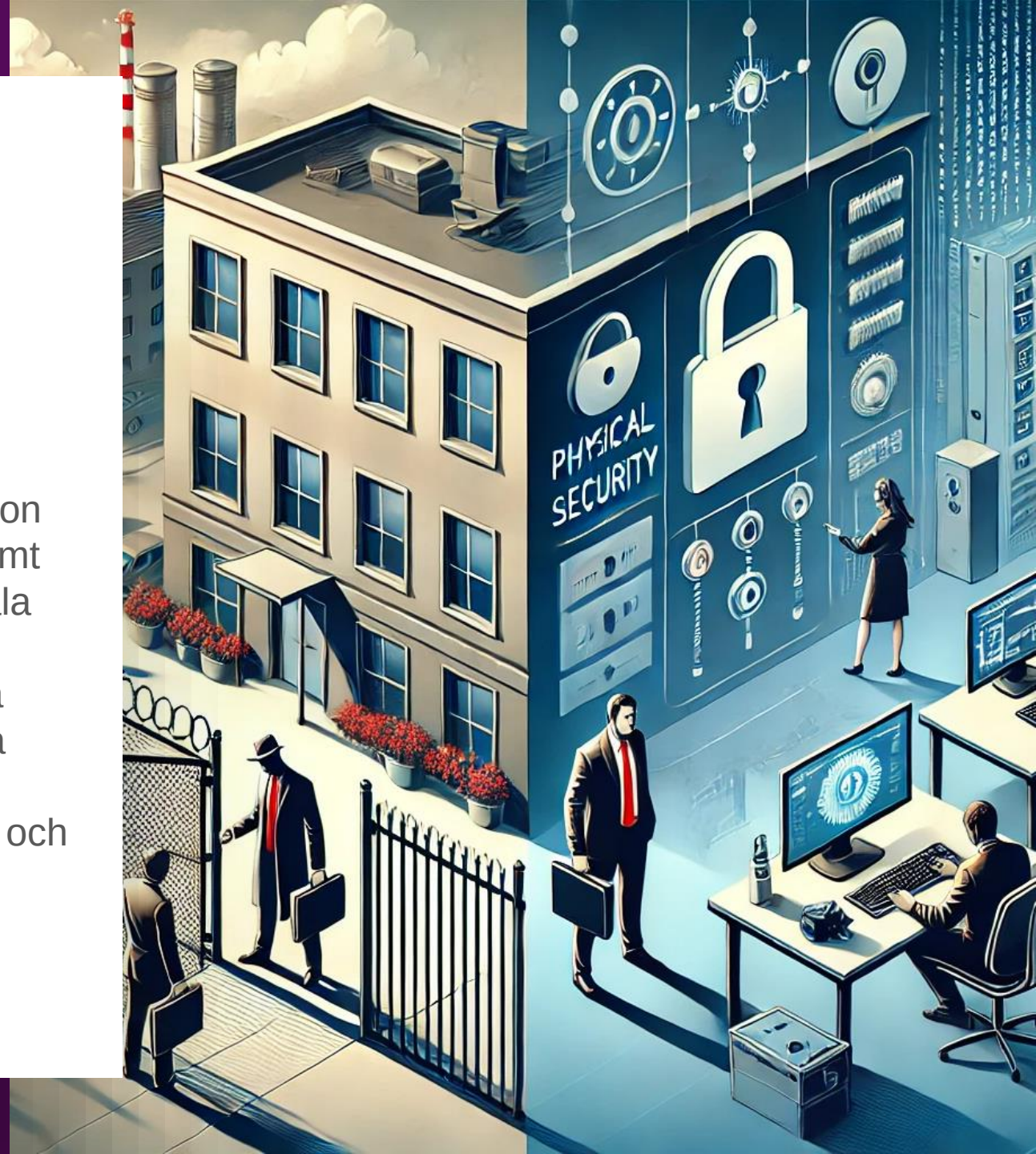
Period: 2025 – 2027

FÖRETAGSSPECIFIKA INSATSER

FYSISK & DIGITAL SÅRBARHET

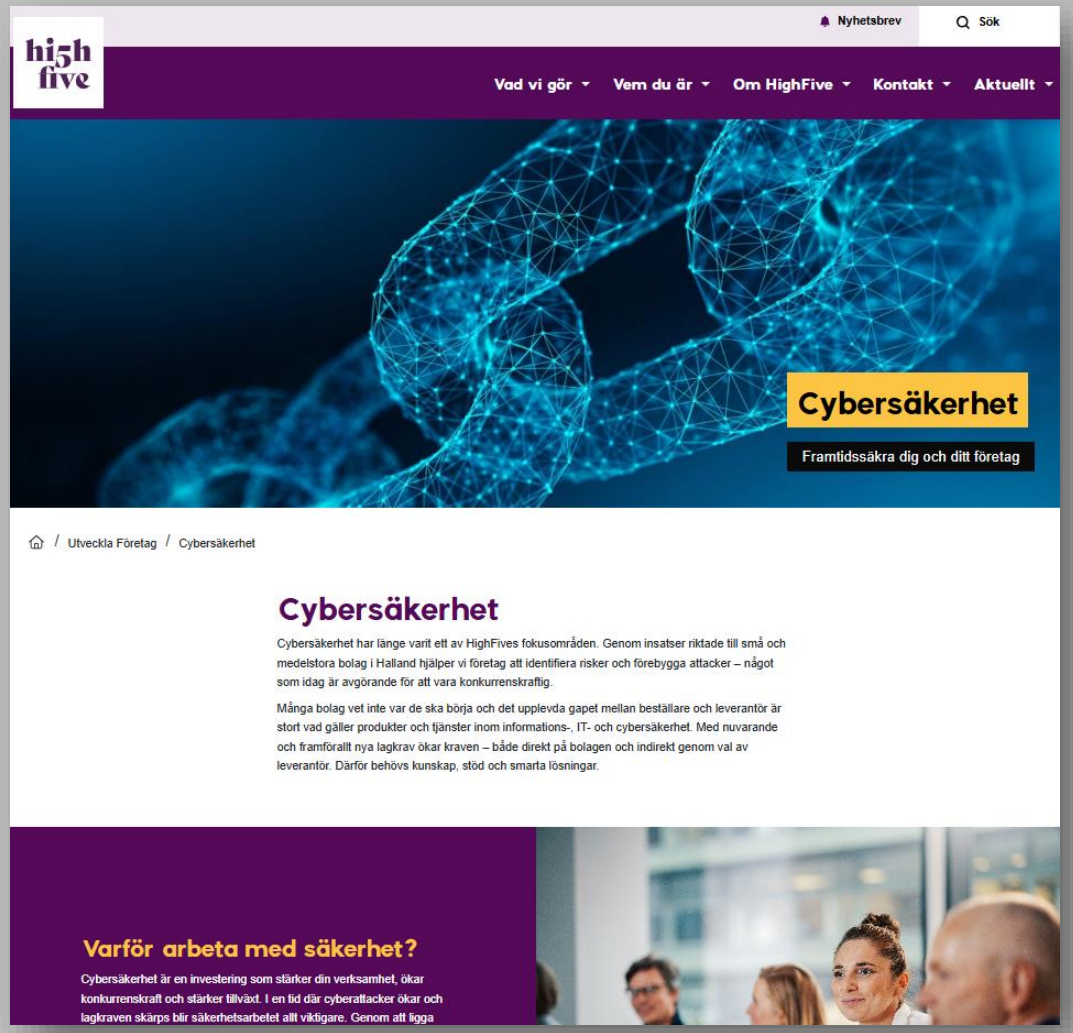
Aktiviteten som utförs av studenter från Högskolan handledda av en extern expert består av två kompletterande insatser i form av en fysisk inspektion av arbetsställe som bygger på en ISO-standard, samt en automatiserad sårbarhetsscanning av den digitala miljön. Detta kommer mynna ut i en rapport med förbättringar för det berörda bolaget. Aktiviteten ska också möta projektmålet om en ökad säkerhetsnivå men även att öka entreprenörskap hos framförallt studenter i Halland för att möta näringslivets behov och samtidigt behålla kompetens i regionen.

Deltagande bolag: 50
Period: 2025 – 2027



Läs mer på vår webb:

[Cybersäkerhet | HighFive Innovationsarena]



Sugna på att vara med?
Kontakta oss idag!

PROJEKTLEDARE

Fredrik Larson

0763493728

fredrik.larson@highfive.se

@fredriklarson

AI och juridiken

Vem är jag?

Jurist inom IT-rätt och utbildad inom informationssäkerhet

Specialiserad på dataskydd (GDPR), cybersäkerhet, informationssäkerhet och internrevision enligt ISO27001.

Rådgivande konsult inom GRC

Säkerhetskonsult med fokus på strategi – hjälper till med riskbedömning, strategier och prioritering. Kortsiktigt som tillfällig konsult eller långsiktigt som exempelvis CISO.

Jobbar även med rådgivning inom regelefterlevnad genom att hjälpa organisationer att förstå och uppfylla lagkrav som GDPR, NIS2, DORA och cybersäkerhetslagen.

ELMHAV SWEDEN

Dagens föreläsning

01 AI-Act – om lagen och dess syfte

02 Vilka omfattas

03 Vilka krav och när de börjar gälla

04 Lagen och annan lagstiftning

05 Praktiska tips

ELMHAV SWEDEN

AI Act är en **EU-förordning** som syftar till att säkerställa att AI är säker, förutsägbar och respekterar mänskliga rättigheter.

Den gäller som **lag i hela EU, inklusive Sverige** och behöver inte implementeras genom nationell lag. Men vissa kompletteringar behövs – exempelvis vilka myndigheter som får tillsynsansvar.

AI-system är *"ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi, som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, på grundval av de indata det tar emot, drar slutsatser om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras."*

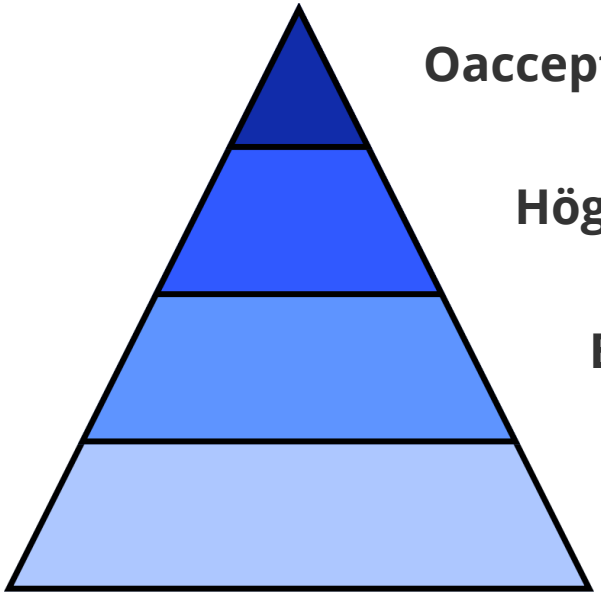
ELMHAV SWEDEN

Vilka omfattas av AI-Act?

- **Verksamheter som utvecklar AI?**
- **Verksamheter som tillhandahåller AI till kunder?**
- **De som använder AI i sin verksamhet för att fatta beslut som påverkar individer eller samhällsviktiga funktioner?**

ELMHAV SWEDEN

AI Act
och de olika risknivåerna



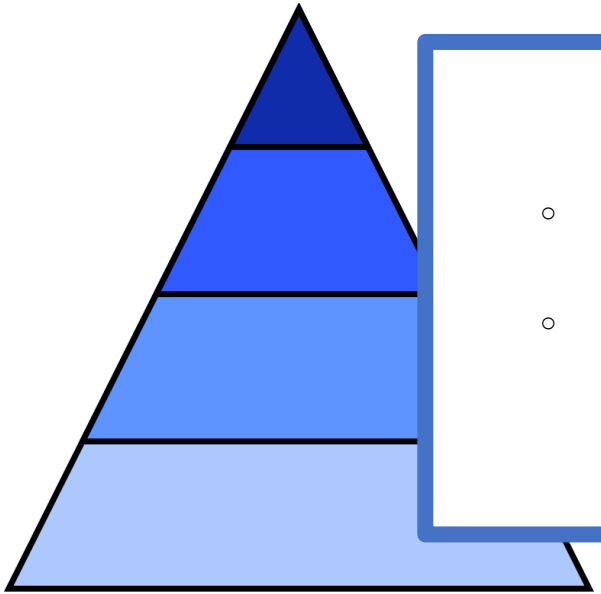
Oacceptabel risk

Hög risk

Begränsad risk

Minimal risk

AI Act
och de olika risknivåerna

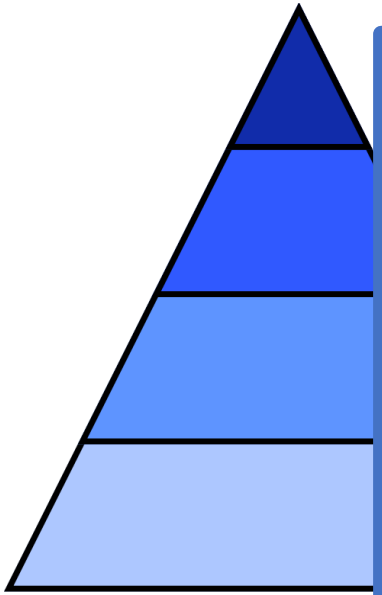


Oacceptabel risk

- Definition: AI som utgör ett klart hot mot människors säkerhet, frihet eller rättigheter.
- Ex: Social scoring, AI som manipulerar barn, ansiktsigenkänning i realtid i offentliga miljöer

Fr.o.m. Februari 2025

AI Act
och de olika risknivåerna

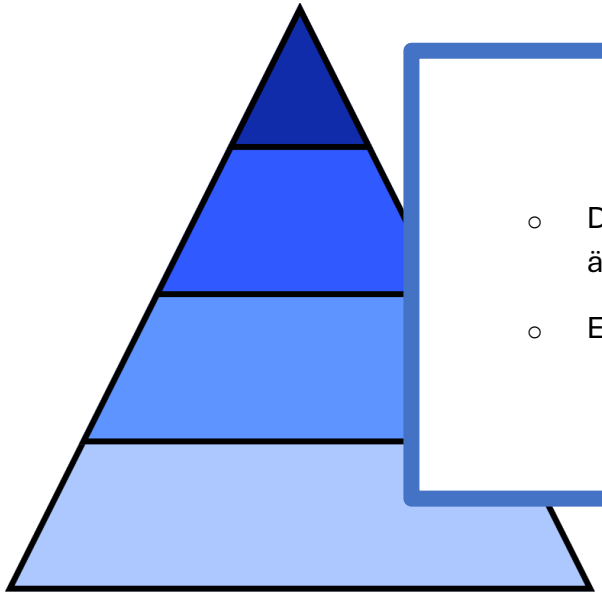


Hög risk

- Definition: AI som används i känsliga samhällsfunktioner där fel kan leda till stora konsekvenser.
- Ex: AI för att sortera jobbansökningar, AI i medicinteknik eller självkörande fordon, AI som påverkar utbildning, rättssystemet, eller kreditgivning.

Fr.o.m. Augusti 2026

AI Act
och de olika risknivåerna



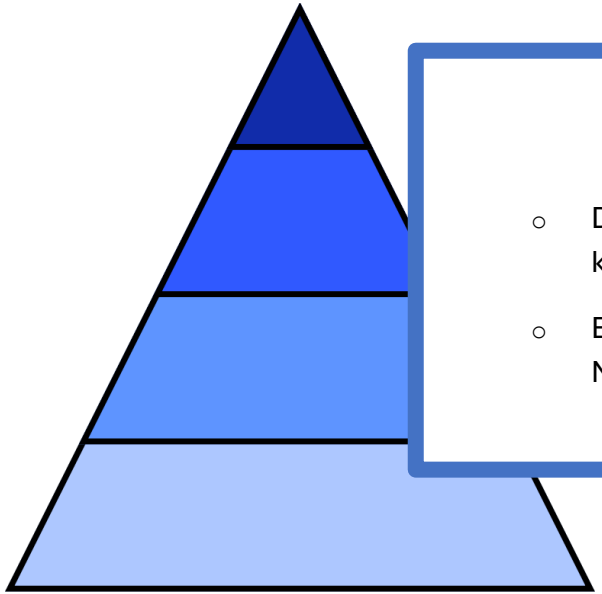
Begränsad risk

- Definition: AI som kan vilseleda användare om det inte är tydligt att det är en maskin.
- Ex: Chatbots, röstassistenter, deepfakes

Fr.o.m. Februari 2025

Minimal risk

AI Act
och de olika risknivåerna



Minimal risk

- Definition: AI som inte påverkar människor i någon känslig roll eller funktion.
- Ex: AI i stavningskontroll eller rekommendationer på Netflix

Minimal risk

Kraven som införs på högrisk AI?

- **Riskanalys och dokumentation** – Företaget måste visa att man förstått riskerna med AI-systemet och hur de hanteras.
- **Säkerställd datakvalitet** – AI:n får inte tränas på felaktig, snedvriden eller diskriminerande data.
- **Transparens** – Det ska gå att förklara hur AI-systemet fungerar och varför det ger ett visst resultat.
- **Mänsklig övervakning** – Viktiga beslut får inte fattas av AI helt utan mänsklig inblandning.
- **CE-märkning** – AI-systemet måste uppfylla vissa tekniska och legala krav innan det får användas.

Det finns **bilagor i lagen** med en lista över högriskområden (bl.a. bilaga III)

ELMHAV SWEDEN

AI Act och annan lagstiftning

AI Act ersätter inte GDPR, NIS2, produktsäkerhetsregler eller diskrimineringslagar – den **kompletterar dem**.

- GDPR handlar om **skydd av personuppgifter**. AI Act handlar om **hur AI-system ska vara säkra, förklara sina beslut och inte diskriminera**.
- Om AI behandlar persondata måste ni följa **både GDPR och AI Act**.
- Tänk: GDPR säger *"du får inte lagra denna data hur som helst"*, AI Act säger *"om du använder den för att fatta beslut med AI måste du visa hur och varför"*.

ELMHAV SWEDEN

Checklista för företag

01 Kartlägg vilken AI ni använder eller planerar att använda.

02 Bedöm om det är högrisk enligt AI act.

03 Börja dokumentera system, datakvalitet och övervakning.

04 Ha koll på era leverantörer – kommer deras AI att vara godkänd.

05 Utbilda ledning och nyckelpersoner.

ELMHAV SWEDEN

Avslutningsvis

AI Act handlar inte om att förbjuda AI – det handlar om att använda AI **på ett sätt som är tryggt, transparent och rättvist**.

Om ni förbereder er nu får ni ett försprång, hinner göra rätt val och blir mer trovärdiga mot kunder och myndigheter.

ELMHAV SWEDEN

Tack!

Kontaktuppgifter:

Webb: https://elmhav.se/

E-post: tova@elmhav.se

Mobil: 0763 – 400 900

COMBITECH

Deepfakes – Vad är det? Hur skyddar vi oss?

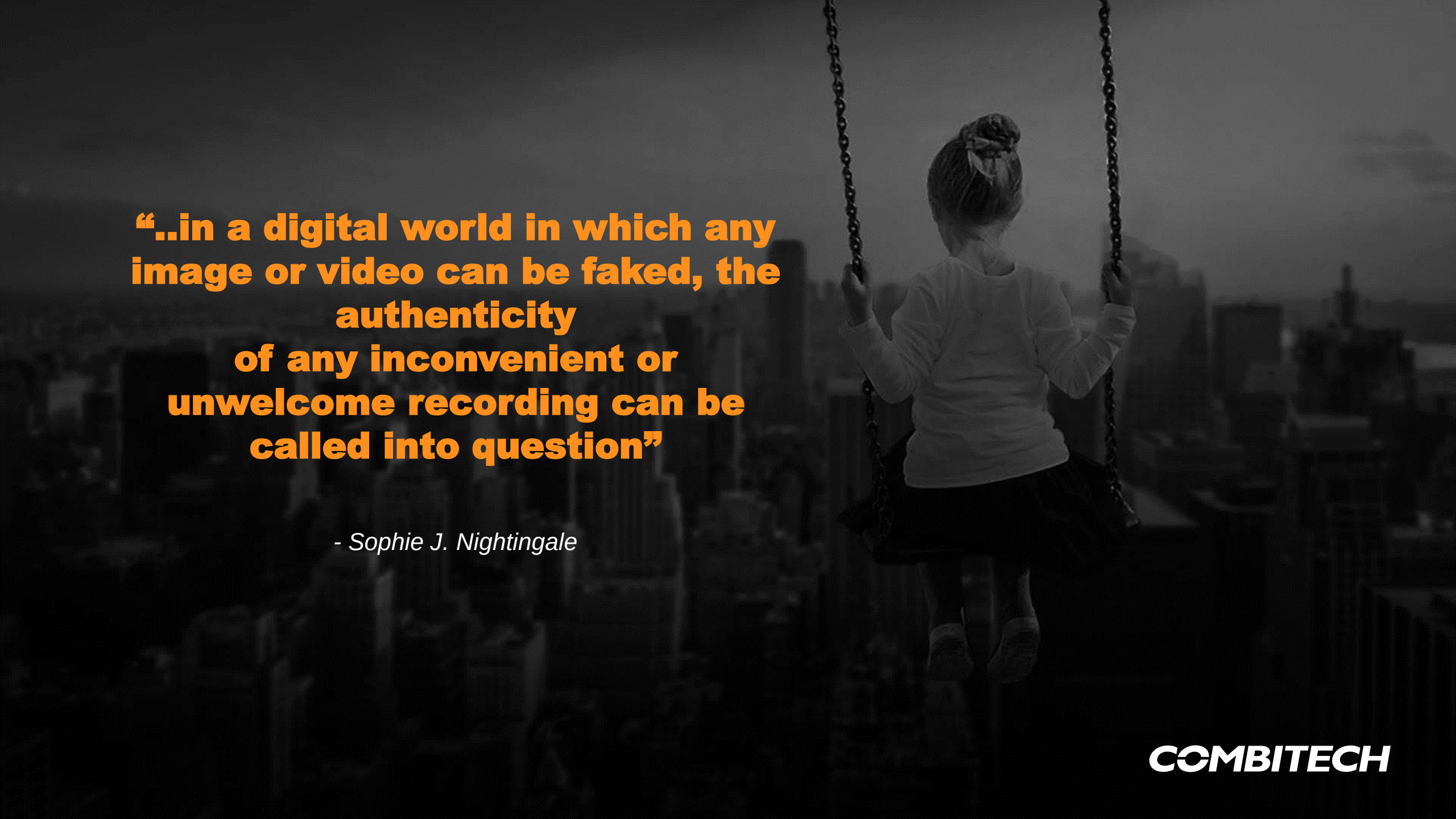
Att möta informationspåverkan & omvärldsanalys
Verktyg för alla verksamheter att kunna upptäcka, hantera och möta påverkanskampanjer och desinformation.

Henrik Ryttergard
Enhetschef & Senior rådgivare
Combitech

CyberSecure Halmstad
2025-05-13

Vem är jag

- **Enhetschef och senior rådgivare inom cybersäkerhet på Combitech och Saab**
- **13 års erfarenhet med fokus på incidenthantering, IT-forensik, penetrationstester och underrättelse**
- **Samhällskritiska verksamheter**
- **Från Halmstad och bor i Halmstad**
- **Bakgrund i försvaret**
- **Pluggat här**
- **Lokalt och globalt**


“..in a digital world in which any image or video can be faked, the authenticity
of any inconvenient or unwelcome recording can be called into question”
- Sophie J. Nightingale
COMBITECH

Vad är en deepfake?

COMBITECH

- **Ett foto, en video eller ljud som skapats med hjälp av AI-teknik för att realistiskt simulera eller ändra personers ansikten, rörelse eller röst**

- **Desto fler referenser det finns**
  Desto bättre blir deepfaken!

- ***Från Hollywood till Photoshop…***
- ***Näää, men med hjälp av en gnutta ny teknik…***

Men vänta – manipulation av foton, video eller ljud är väl inget nytt, eller?
Det har jag sett på tv förr!

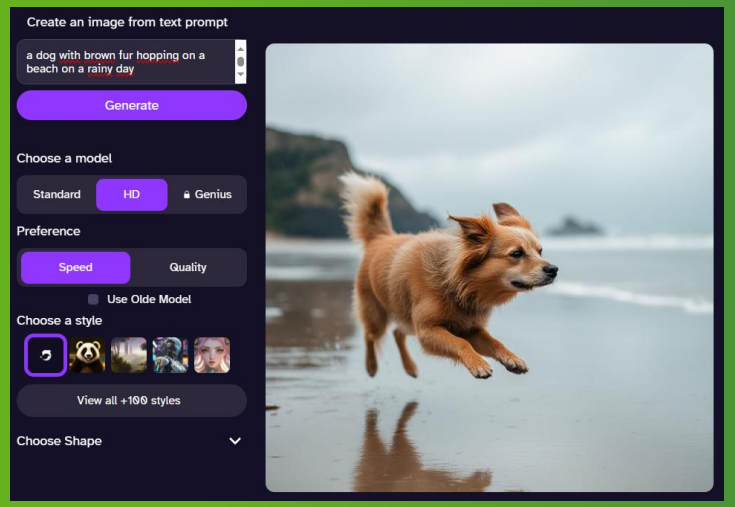
Den nya tekniken

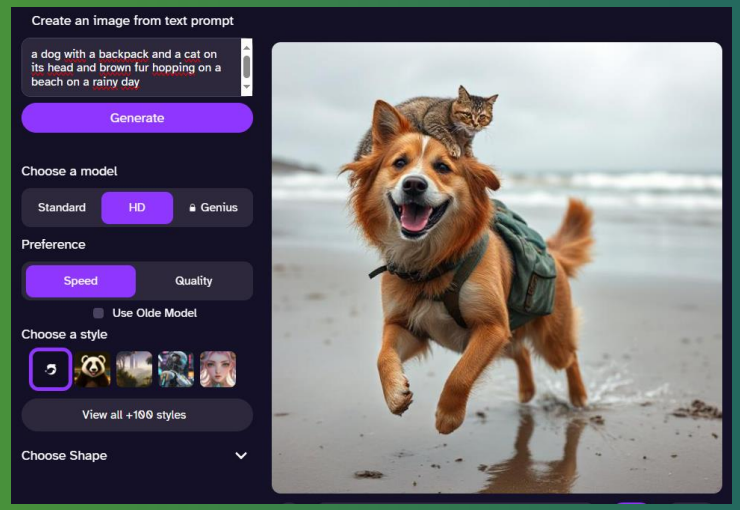
- **Enkel att använda!**
- **Tillgänglig för alla!**
- **Bättre teknik kostar mer!**

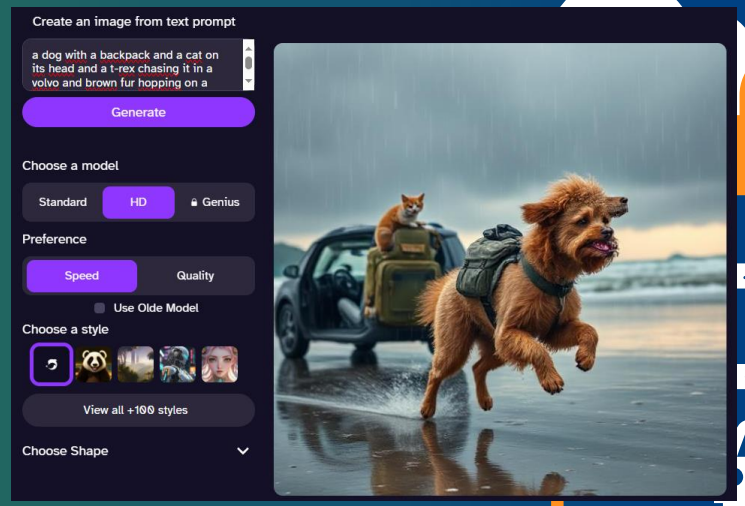
- **Låt oss titta hur enkelt det är att skapa ”Content”**

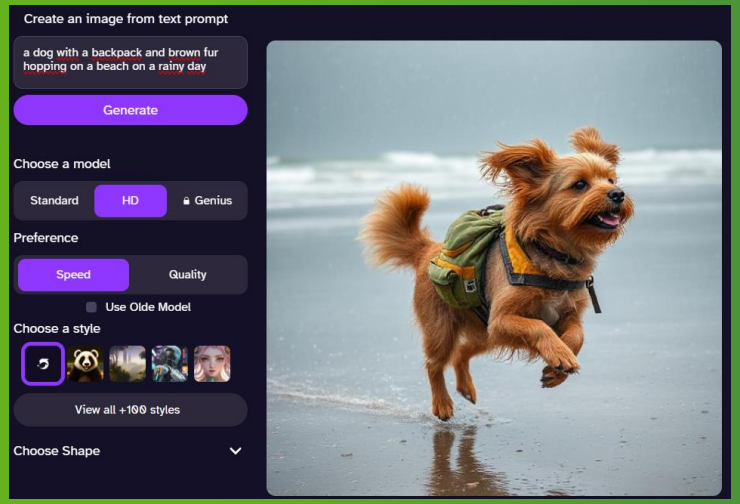
Den nya tekniken

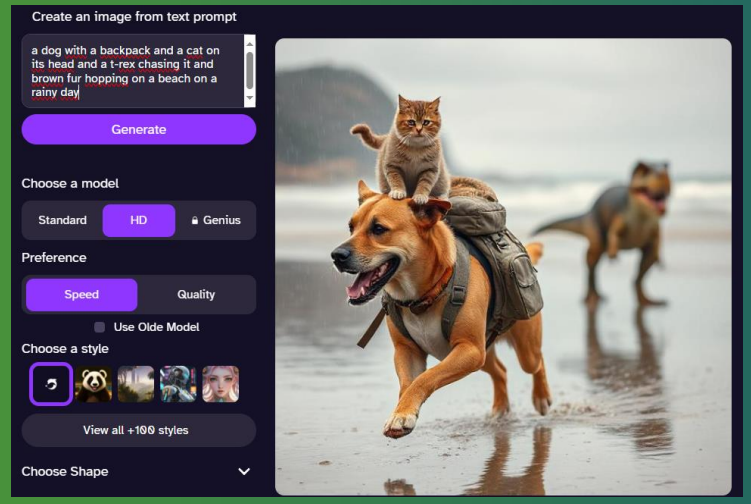
COMBITECH

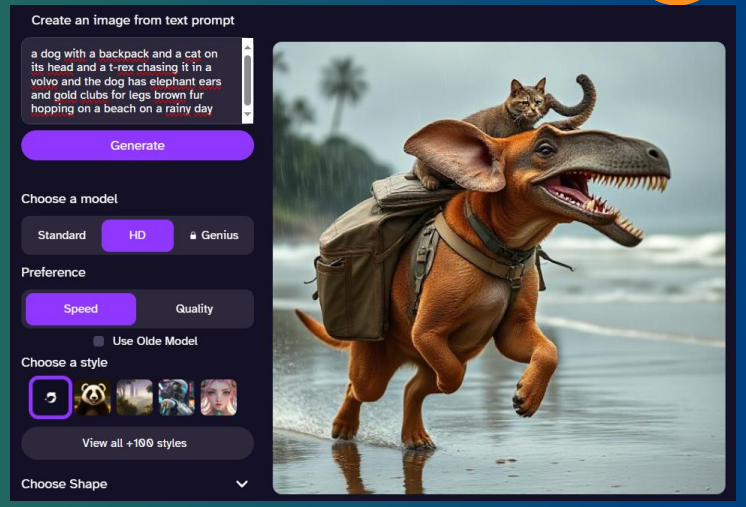












Harmlöst eller skadligt?

Harmlöst eller skadligt?

COMBITECH

Harmlöst eller skadligt?

COMBITECH

Harmlöst eller skadligt?

COMBITECH

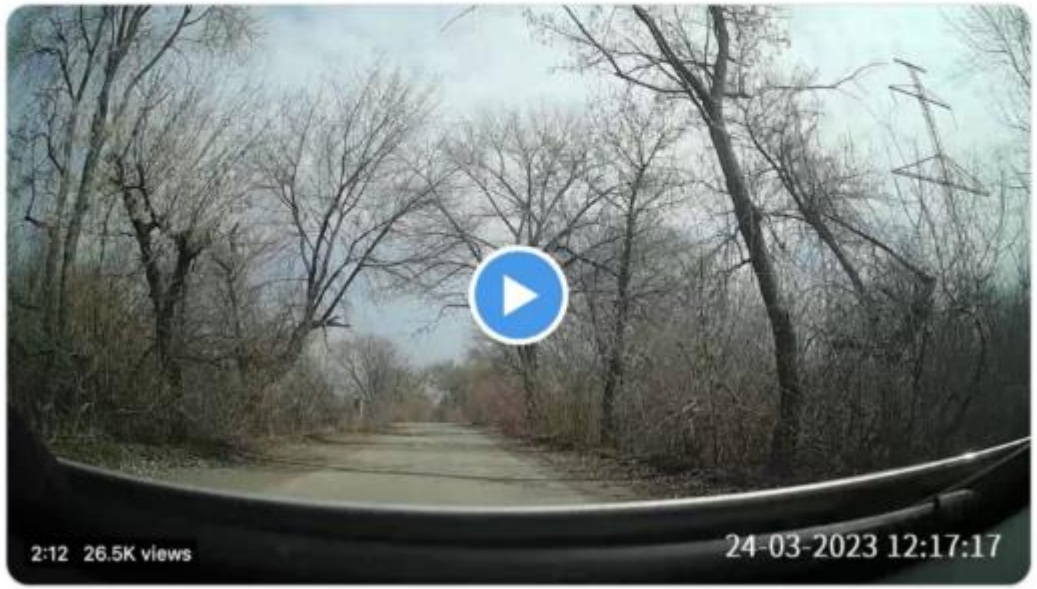
MFA Russia
@mfa_russia
Russia government organization

#Think4Yourself #See4Yourself

Once a Nazi always a Nazi 👇

This is the kind of terror Ukrainians are living in: witness Ukrainian military berate and shoot at a mother with a child in the backseat, calling her "pig" & "scum" simply for... speaking Russian

No Nazis, they say...



1:45 PM · Mar 27, 2023 · **793.6K** Views

959 Retweets **194** Quote Tweets **2,142** Likes

Definitivt skadligt

Definitivt skadligt

- En Pakistansk officerare uttalar sig om vedergällning mot Indien i samband med konflikten under april/maj 2025
- Videon publicerades brett runt om i världen

- Hela videon är dock en deepfake baserat på en annan video…

Innebörden av ”deepfake-content”

- **AI-content & deepfakes kan vara harmlöst och kul**
- **Men är också ett extremt effektivt verktyg för att manipulera och påverka**
- **Ur ett motståndarperspektiv så är deepfakes ren informationspåverkan**

Informationspåverkan 2025

COMBITECH

Aktörer

Stater

Kriminella/
Terror

Konkurrenter

Opportunister

Vem som helst!?

Metoder

Desinformation
(text, audio, video)

Deepfakes
(text, audio, video)

Falska
gräsrotsrörelser
& konton

Marknadsföring och
manipulation - sociala media
och/eller sökmotorer

Symboliska
handlingar

Dataförgiftning

Annonser
Omedveten
finansiering

Leaking & Doxing

Slop

Risker

Försvagat /
smutskastat
varumärke

Minskat förtroende från
allmänhet och kunder

Ekonomiska förluster

Utpressning och
trakasserier

Begränsad förmåga att
leverera varor och tjänster

Informationspåverkan 2025: läget i stort

COMBITECH

- **Informationsmiljön kan liknas vid en spelplan utan linjer, domare och regler**. För varje år blir den alltmer komplex och svårnavigerad. Idag är det utmanande att särskilja legitim opinionsbildning (inklusive satir, lobbyism, samt sälj- och marknadsföring) från illasinnad kommunikation, såsom falska gräsrotsrörelser, statliga medier och proxy-aktörer (både medvetna och omedvetna). Dessutom finns algoritmer som kan "premiera det negativa" eller manipuleras för att göra så.

- **Digitaliseringen driver förändringar över hela samhället,** och det finns ett växande behov av beredskap och skydd, eftersom framsteg medför både möjligheter och risker. Trots att det har gått över 15 år sedan sociala medier blev stort, verkar vi fortfarande yrvaket försöka hantera en situation som ingen riktigt kunde förutse. Det bästa med internet och sociala medier är samtidigt dess värsta aspekt. Möjligheterna att ta del av all världens information, sprida sina budskap och hitta likasinnade gäller tyvärr även för antagonister. Till exempel kan grovt kriminella "marknadsföra" sitt våldskapital på sociala medier.

- **Idag är desinformation (avsiktligt vilseledande eller manipulerad information) en betydande faktor inom de flesta områden.** Den används av antagonister och andra illasinnade aktörer inom exempelvis politik, näringsliv, media, spel, skola, religion och akademi, liksom i det allmänna samtalet.

- **En global industri.** Utvecklingen av omfattningen och spridningen av desinformation, samt möjligheterna att manipulera innehåll på exempelvis sociala medier, är enorm. Idag har en global industri vuxit fram som erbjuder varor och tjänster för spridning av ogrundad information. Detta innebär att i princip vem som helst kan genomföra en storskalig och avancerad påverkanskampanj.

- **"Alla ljuger!"** Det handlar inte bara om "vi mot dem". Även om de allra flesta har goda intentioner, måste vi vara medvetna om att många använder vilseledande och felaktig information för att nå sina ekonomiska och politiska mål. Det är betydligt fler än de "onda" som gör detta. Det inkluderar västländer, näringsliv och privatpersoner.

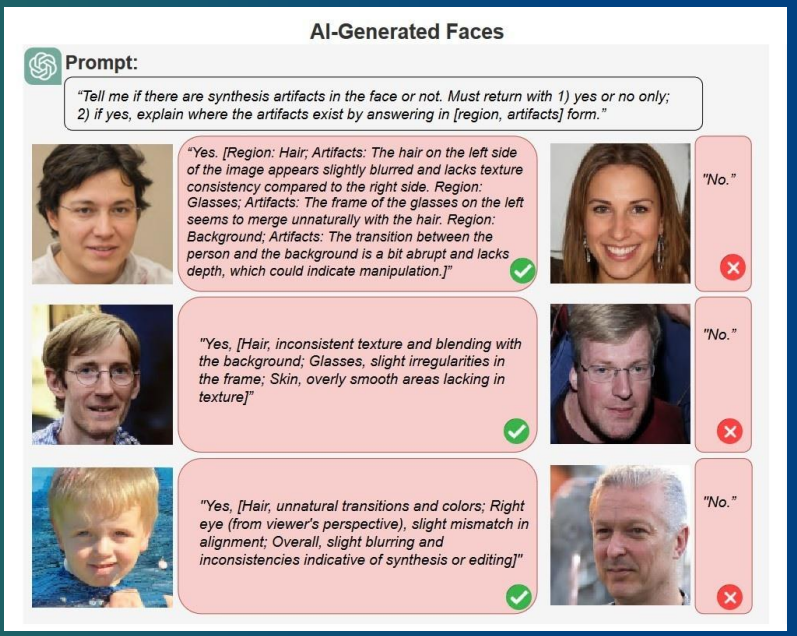
- **Risker med begreppet desinformation.** En risk är att vi drar alla synpunkter som vi inte uppskattar över en kam och benämner dem som "desinformation", något som har blivit allt vanligare. Ofta använder aktörer begreppet desinformation som ett operativt verktyg. I sådana fall bör de kunna argumentera för hur de anser att det skiljer sig från yttrandefrihet, annars riskerar resonemanget att bli rundgång. Om man definierar desinformation som avsiktligt falsk eller vilseledande information, faller den fortfarande inom ramen för yttrandefrihet. Det krävs dock ett ställningstagande kring när och hur det är lämpligt att bemöta sådan information.

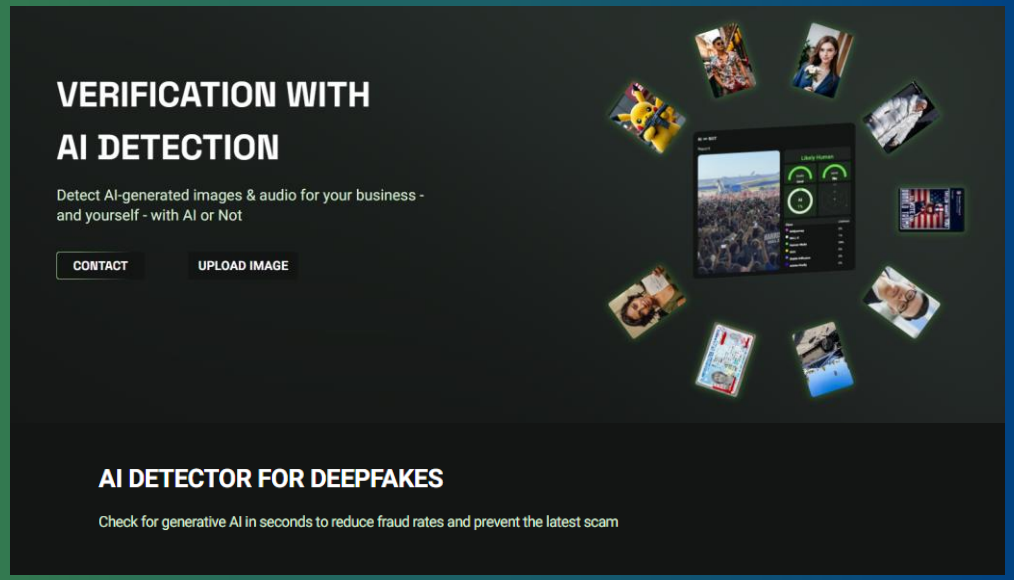
- **Från sci-fi till verklighet. Det som igår var science fiction är idag det normala.** Utvecklingen av generativ AI, såsom stora språkmodeller (LLM), är verkligen fantastisk. Men baksidan är att vi har gett alla – inklusive illasinnade aktörer – "möjligheten att hälla obegränsat med bensin på sin eld". Vi befinner oss nu i en gråzon med hundra nya nyanser. Hur ser vi egentligen på användningen av syntetisk media? Är det acceptabelt att aktörer inom försäljning, marknadsföring eller rekrytering använder sig av syntetiska profiler? Är det okej att politiker svartmålar sina motståndare med hjälp av tekniken? Detta kräver att vi tar ställning och reflekterar över de etiska och praktiska konsekvenserna.

- **Utvecklingen gör det tydligt att informations-påverkan inte enbart handlar om "motståndaren" utan även om samhället och medborgarna.** Utgångspunkten för alla verksamheter bör vara: hur ska vi förstå våra målgruppers behov och intressen för att skapa rätt förutsättningar att möta dem? Illasinnade aktörer är skickliga på målgruppsanalys, men de tar inte hänsyn till målgruppens intressen och förutsättningar utan exploaterar deras sårbarheter. Det är en viktig nyansskillnad här, som skiljer det vi ska göra från det som "motståndaren" gör.

Ta med er

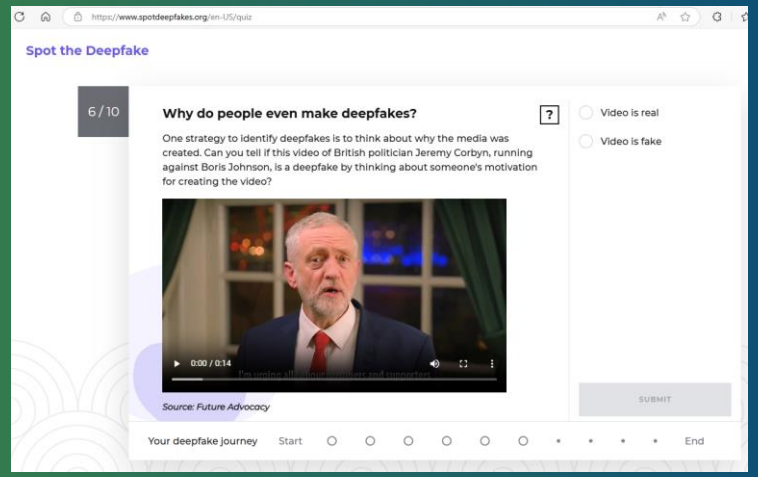
- **Syntetisk media kommer bli mycket mer vanligt**
- **Med hjälp av AI kan content skapas extremt snabbt som också ser väldigt äkta ut!**
- **AI kan även användas för att upptäcka och motverka, använd det klokt!**

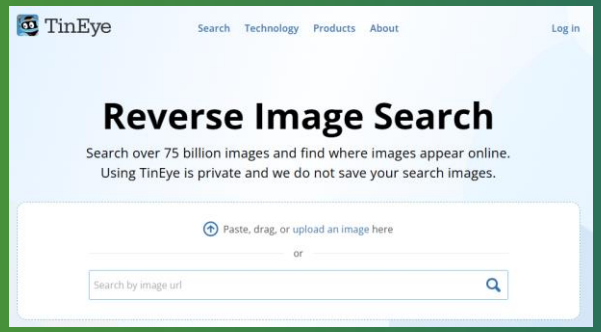


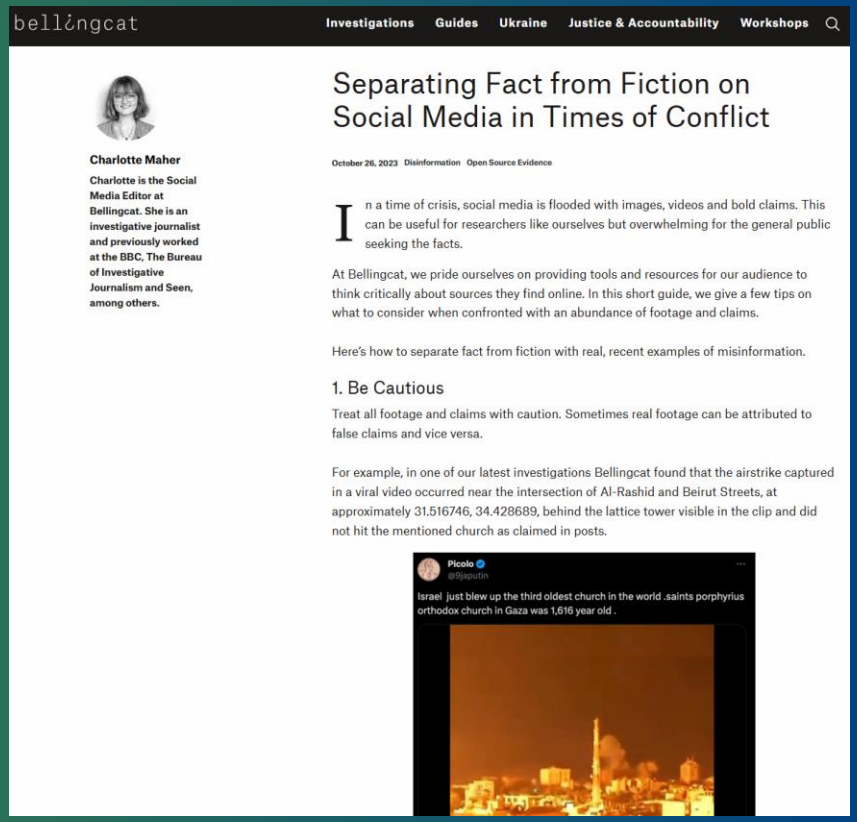


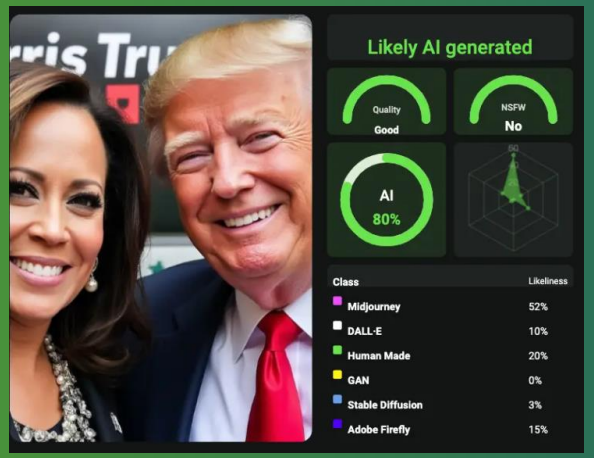
Ett par riktigt vassa tips!

- **Spot the deepfake – https://www.spotdeepfakes.org/**
- **Tineye Reverse image search - https://tineye.com/**
- **Bellingcat - https://www.bellingcat.com/resources/how-tos/2023/10/26/separating-fact-from-fiction-on-social-media-in-times-of-conflict/**
- **AI or Not - https://www.aiornot.com/**









Ta med er

- **1 – Var försiktig**
  Behandla all ni ser och hör med försiktighet.
  Var inte rädd för det men var kritisk till det

- **2 – Upprör innehållet eller budskapet dig?**
  Om innehållet eller budskapet påverkar dig eller upprör dig, då är det extra stor risk att någon skapat detta just för att väcka känslor
  Ofta negativa sådana som hat, rädsla eller avsky.

- **3 – Tänk kritiskt!**
  Det är som sagt inte svårt att manipulera varken bild, video eller ljud. Ju mer underlag det finns för att skapa content kring en individ desto lättare är det att få det mer verkligt

- **4 – Kontrollera källan**
  Ansvarsfulla analytiker, journalister eller politiker delar sina källor.
  Bara det faktum att det saknas källor borde vara något som får er att tänka till extra mycket

- **5 – Samma plats behöver inte betyda samma incident!**
  Bilder och videos får ofta ”nytt liv” när något händer på samma plats vid ett annat tillfälle.

- **6 – ”Häng med” gällande ny teknik, AI och manipulation**
  Dagens teknik kan snabbt skapa trovärdigt material och framtidens teknik kommer kunna göra det här ännu bättre. Det viktiga är att ni skaffar er kunskap om vad som kan göras för att ni sen skall kunna skydda er emot det.

- **7 – Var försiktig med statsaktörer**
  Vi i Sverige glömmer lätt bort hur bra vi har det. Vi lever i en rättsstat med hög nivå av transparens och låg korruption. Däremot är flertalet andra stater inte sådana.
  Med en hel statsapparat och nästintill oändliga resurser kan mycket mer material produceras för att uppnå sitt mål.

- **8 – Även etablerade organisationer och journalister gör fel ibland**
  Det är inte alltid så att de som publicerar eller delar material håller med om det utan de rent av bara delar eller rapporterar om det. Alla kan göra fel och det är hur dem och vi hanterar det efteråt som är viktigt

- **9 – Vårda din mentala hälsa**
  Att gräva ner sig i kaninhålet timme efter timme samtidigt som innehållet kan vara svårt att smälta är tufft för psyket. Glöm inte bort dig själv under tiden!

Rekommenderade verktyg

– Utbildningar, spel, handböcker, rapporter och nyhetsbrev.

Utbildning

COMBITECH

Kurser och material

- Webbutbildning informationspåverkan, MSB
- Utbildning | Myndigheten för psykologiskt försvar
- DigResiliens - Utbildningar och kurser | RISE
- Training & Vaccine Insights hub, First Draft
- MIK Kunskapsbank
- Fojo Faktajouren
- Bli inte lurad, MPF
- Kunnig på nätet - förstå informationspåverkan | RISE
- Utbildning för motståndskraft Lunds Universitet
- The role of narrative in misinformation games | HKS Misinformation Review

Spela ett spel!

- Spot the Deepfake
- Bad News
- Go Viral
- Nyhetsvärderaren (nyhetsvarderaren.se)
- fakey.osome.iu.edu
- Spotting Misinformation + Disinformation
- Cat Park

Våra favoriter:

DigResiliens - Utbildningar och kurser | RISE

Våra favoriter:

MIK Kunskapsbank

Våra favoriter:

Spot the Deepfake

Bad News

Högskolekurser

- Informationsmiljön – grundkurs – Försvarshögskolan
- Politisk kommunikation: Informationspåverkan som säkerhetsproblem
- Social Media, Disinformation and Fake News, 7.5 Credits - Örebro University
- Desinformation och psykologiskt försvar | Karlstads universitet
- Riskperception och informationspåverkan | Karlstads universitet
- Medier, desinformation och propaganda: Att navigera i det offentliga samtalet | Göteborgs universitet

Diplomutbildningar

- Upptäck, förstå och möt informationspåverkan – Sveriges kommunikatörer
- Totalförsvar för kommunikatörer - Sveriges kommunikatörer
- Skydd mot informationspåverkan - ett strategiskt helhetsgrepp – Företagsuniversitetet
- Säkerhetshot och scenarioplanering - kurs – Företagsuniversitetet
- Kurser | Kairos Future

Handböcker och vägledningar

COMBITECH

Informationspåverkan (inkl. hybrida hot)

- Att möta informationspåverkan – Handbok för journalister (mpf.se)
- Bli inte lurad - Handbok för privatpersoner | Myndigheten för psykologiskt försvar
- RESIST Counter Disinformation Toolkit, GCS
- Handbok debunking 2020
- The Conspiracy Theory Handbook
- Psychological Defence: Concepts and principles for the 2020s | Myndigheten för psykologiskt försvar
- Building Resilience and Psychological Defence - An analytical framework for countering hybrid threats and foreign influence and interference |
- Rättsligt ramverk för bemötande av informationspåverkan
- What is the Diamond Model of Intrusion Analysis?
- Strategisk verktygslåda mot hybridhot. Ett ramverk för gemensam problemförståelse

Våra favoriter:

CORE_comprehensive_resilience_ecosystem

Våra favoriter:

Handbok debunking 2020

Våra favoriter:

RESIST Counter Disinformation Toolkit, GCS

Strategisk- kris- & riskkommunikation

- Kriskommunikation i samverkan
- Vägledning för kommunikation under kriser : Forskningsbaserade metoder med fokus på beteendeförändring,
- Nya vägar för risk- och kriskommunikationen
- Försvarsvilja och gemenskap - Om betydelsen av förtroende och demokrati för försvarsviljan

Övrigt

- Sveriges Radio Sociala medier
- ChatGPT - Skydd mot informationspåverkan
- Introducerar Cicero-GPT – psykologiskt försvar.
- STORM

Omvärldsanalys och framsyn

COMBITECH

OSINT

- Bendobrown – YouTube
- OSINT Toolkit | Links To Digital Tools Used By Researchers (comskills-ukraine.co.uk)
- Welcome to ObSINT! | ObSINT
- Bellingcat Open Source Toolkit
- Google Alerts – bevaka intressant nytt innehåll på internet
- Social Media Monitoring: A Primer, Stratcom
- Social Media Monitoring Tools: An In-Depth Look, Stratcom

Lägesbild & analystekniker

- Samlad lägesbild, MSB
- Pandora Forward Looking Cell
- DISARM Framework
- Metodguide Strukturerad brainstorming | Göteborgsregionen (GR) (goteborgsregionen.se)
- Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community

Våra favoriter:

Futures toolkit for policymakers and analysts - GOV.UK

Våra favoriter:

Bendobrown – YouTube

Våra favoriter:

Bellingcat Open Source Toolkit

Scenarier

- Scenarier och typfall - Totalförsvarets forskningsinstitut - FOI
- Riskkatalog (msb.se)
- Scenarier – ett effektivt sätt att hantera framtiden

Framsyn, strategi & transformation

- Hur utforskar vi framtiden med strategisk framsyn? | Vinnova
- Strategic foresight | VTT
- AnticipaTech - deftech | Defence Future Technologies
- Copenhagen Institute for Futures Studies
- Framåtblickande omvärldsanalyser - Hur gör andra?
- Futures toolkit for policymakers and analysts - GOV.UK
- Omvärldsanalys-på-kort-och-lång-sikt_19Maj03_V2-003.pdf
- Partnerskapet LOFT – ett kommunledningspartnerskap
- Rådighet för transformation - mitt anförande på Folk och Försvars rikskonferens i Sälen - Carl Heath
- Glimt - vårt nya vapen i kampen för Ukrainas frihet - Totalförsvarets forskningsinstitut - FOI

Omvärldsanalys & framsyn

COMBITECH

Nyhetsbrev, löpande monitorering och fact checking

- SVT Verifierar | SVT Nyheter
- BBC Monitoring Essential Media Insight
- Samtalet om Sverige , Svenska institutet
- DisinfoDocket
- The Record from Recorded Future News
- EUvsDisinfo | Detecting, analysing, and raising awareness about disinformation – EUvsDisinfo
- EDMO – United against disinformation
- Forsiden – faktisk
- Kallkritikbyran
- Källkritik, fake news och faktagranskning | Facebook

Prenumerera på Anton Lifs nyhetsbrev!

Våra favoriter:

Threat Intelligence Blog | Recorded Future

Våra favoriter:

DisinfoDocket

Våra favoriter:

Källkritik, fake news och faktagranskning

Myndigheter, tankesmedjor och företag

- Startsida - Krisinformation.se
- DFRLab - DFRLab
- EU DisinfoLab
- Publikationer | Myndigheten för psykologiskt försvar
- Threat Intelligence Resources | Recorded Future
- StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia
- Hybrid CoE - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats
- Graphika
- Mandiant Threat Intelligence | Google Cloud
- Home – ISD
- Center for Countering Digital Hate | CCDH
- The Global Disinformation Index

Rapportera – 8 frågor

Kort beskrivning av händelse och informationen

1. Hur upptäcktes händelsen? I vilket forum/media?
2. Varför misstänker ni att det har koppling till en antagonist?
3. Går det att identifiera ett syfte bakom informationen?
4. Går det att se några tydliga effekter redan nu av informationen?
5. Hur stor är spridningen?
6. Hur påverkar händelsen organisationens förmåga att utföra ert uppdrag?
7. Hur påverkar händelsen aktörer som är beroende av ert uppdrag, och/eller den generella allmänheten?
8. Har åtgärder vidtagits? Hur och varför?

COMBITECH

Shaping a smart and resilient society

Henrik.Ryttergard@combitech.se
+46 734 37 20 53