COMBITECH

Verktygslåda

Att möta informationspåverkan & omvärldsanalys

Ett försämrat säkerhetsläge medför ett ökat behov för alla verksamheter att kunna upptäcka, hantera och möta påverkanskampanjer och desinformation.

Version 2026-04-08

Informationspåverkan 2026

COMBITECH

Aktörer

Stater

Kriminella/
Terror

Konkurrenter

Opportunister

Vem som helst!?

Metoder

Desinformation
(text, audio, bild, video)

Deepfakes
(text, bild, audio, video)

Falska
gräsrotsrörelser
(inkl. AI-agenter)

Marknadsföring och
manipulation - sociala media
och/eller sökmotorer

Symboliska
handlingar

Dataförgiftning

Slop
”Slask/sörja”

Annonser
Omedveten
finansiering

Leaking & Doxing
*”Släppa känsliga
dokument”*

Risker

Försvagat /
smutskastat
varumärke

Minskat förtroende från
allmänhet och kunder

Ekonomiska förluster

Utpressning och
trakasserier

Begränsad förmåga att
leverera varor och tjänster

Informationspåverkan 2026: 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.

Imorgon kan ”AI svärmar” användas för att skada det demokratiska samtalet!?

COMBITECH

2020

År 2019 lanserade OpenAI GPT-2, föregångaren till ChatGPT. Redan vid lanseringen varnade ledande experter för att syntetisk media skulle bli en betydande utmaning inom kognitiv påverkan.

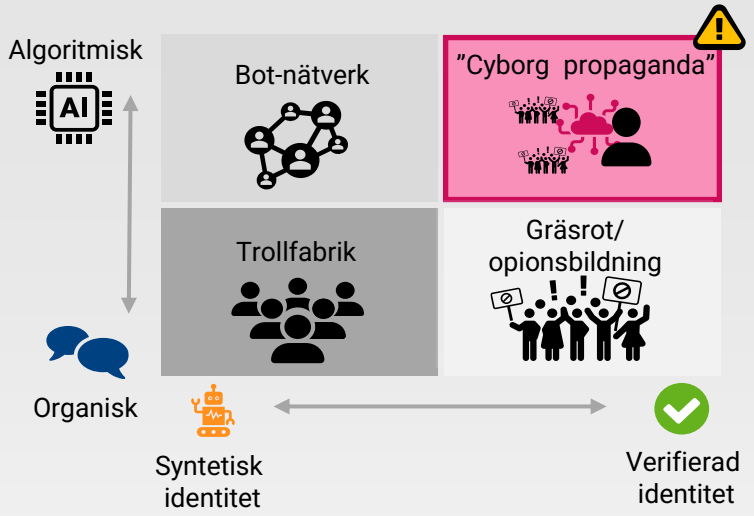
Uppmärksamheten riktades främst mot deepfakes i form av video och bild men flera varningssignaler pekade på att just syntetisk text riskerade att bli särskilt svårhanterlig.

Flertalet studier bekräftade att vilseledande information kunde spridas i stor omfattning och vara svår att upptäcka eller särskilja från äkta material. En studie visade till exempel att läsare ofta bedömde GPT-2-genererade nyhetstexter för äkta, nästan lika ofta som texter från etablerade mediehus.

Trots detta betraktades generativ AI och syntetisk media av den breda allmänheten mest som science fiction.

> ” Synthetic video and audio seemed pretty bad. Synthetic writing - ubiquitous and undetectable - will be far worse”
>
> – *Renee DiResta*

2026



Under 2024 blev AI-assistenter vardag, plötsligt kunde vem som helst skräddarsy sin egen chatbot. De har stöttat oss i vardagen, men också gett kriminella, opportunister och främmande makt nya verktyg. Från 2025 har AI-agenter fått allt större uppmärksamhet och under 2026 ser det ut att bli allt vanligare, sannolikt blir det norm att både individer och organisationer utvecklar och integrerar agentlösningar i sina arbetsflöden. Tidigare var skala ofta en tröskel för hotaktörer. Nu när enorma mängder vilseledande och/eller skräddarsytt innehåll kan produceras, anpassas och spridas till minimal kostnad har informationsmiljön fått helt nya spelregler:

20XX

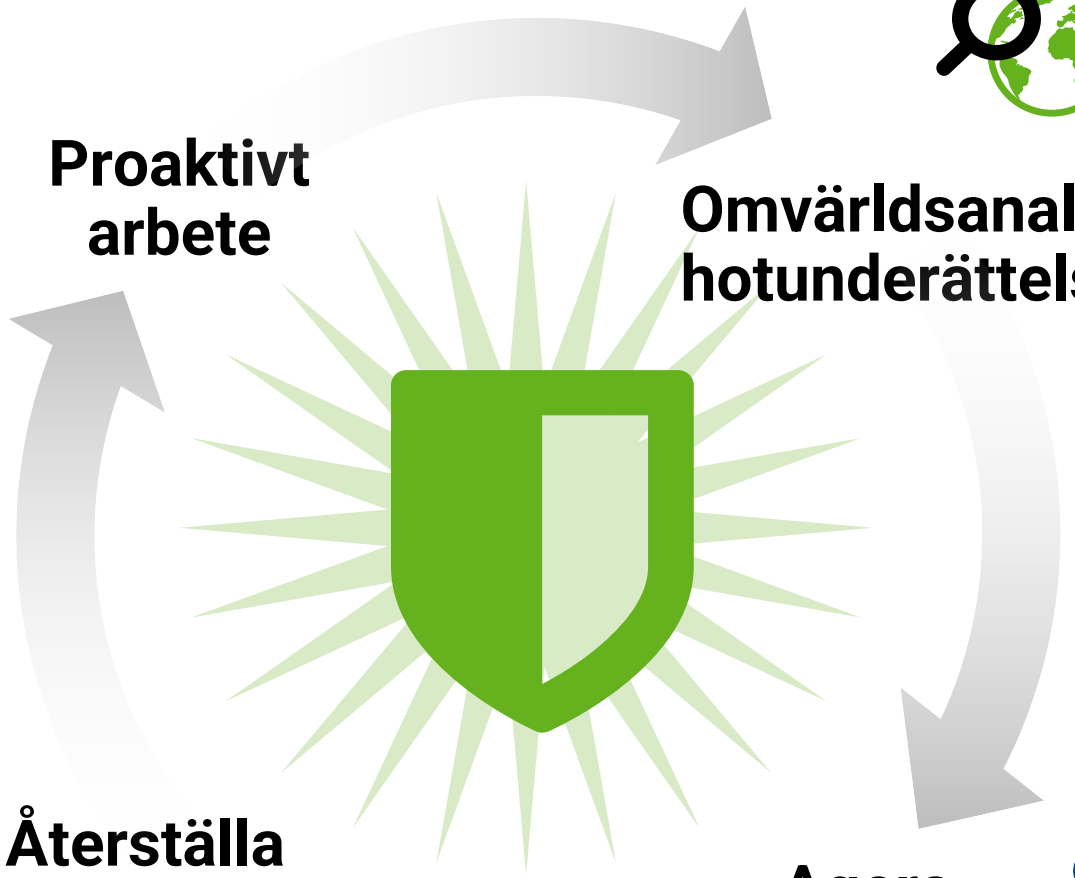
Nästa steg i utvecklingen kan vara ”AI-svärmar”. Illasinnade AI-svärmar är samordnade nätverk av AI-styrda konton och personas som påverkar våra (digitala) samtal. Till skillnad från enkla copy-paste-botar kan de efterlikna riktiga användare och agera långsiktigt. System som sannolikt inte enbart kommer att kunna besvara artiklar, inlägg och kommentarer i textbaserade forum, utan även generera bilder, ljud och andra uttrycksformer dynamiskt – för att förstärka narrativ och skapar ökad trovärdighet. Ett exempel är (syntetisk) konsensus, där många ”AI-personas” skapar en falsk känsla av bred enighet.

Våra rekommendationer

Helhetstänk och tio rekommendationer

Helhetstänk - så bygger vi motståndskraft

COMBITECH



En Personlig brandvägg

Framsyn & scenarioanalys

Säkerhetskultur

Strategisk- & Riskkommunikation

Riskhantering säkerhetsskydd

Övning & red team

Erfarenheter & utveckling

Action Reviews!

Fokus & prioritering

Verktyg

Möjliga hot & sårbarheter

Bedöma

Standardisera (ex. incidentrapport)

Kommunicera och dela

Hantera/försvara

10 Rekommendationer

COMBITECH

1 Proaktivitet

- **Tidig information:** Informera fler kollegor och andra intressenter tidigt, om ert arbete kring förmåge-byggande och krishantering - för att bygga medvetenhet och förkorta framtida ledtider.
- **Proaktiv delning:** Sänk tröskeln för informa-tionsdelning internt och externt.
- **Teknik & beteende:** Öka fokus på innovation. Inkludera beteende-kommunikation och teknik, så som Generativ AI och COM-B, för förbättrad risk- och kriskommunikation. För att stödja önskade beteendeförändringar.

2 Lägesförståelse

- **En gemensam grund:** Genomför en översyn av hur verksamheten, enskilt och tillsammans med andra, kan stärka sin förmåga till läges-förståelse – en gemensam förståelsegrund, med fokus på hybrida hot, så som informationspåverkan.
- **Öka er medvetenhet** kring allmänna såväl som specifika risker, sårbarheter och hot.
- **Sverigebilden:** Fördjupa er kunskap om Sverigebilden och hur ni, liksom egen sektorn/ bransch uppfattas.

3 Framsyn

- **Satsa på framsyn:** Framsyn (Foresight) handlar om att förbereda organisationen för oväntade händelser, samt att främja en kultur av kontinuerligt lärande och anpassning.
- **Integration av strategi:** Genom att tydligare integrera framsyn i organisationens strategiarbete kan vi bättre navigera i nuvarande verklighet och aktivt påverka framtiden
- **Arbeta med scenarioanalys och scenarioplanering:** Skapa scenarion som ger planeringsunderlag för olika utvecklingar. Väntade liksom oväntade.

4 Proaktiv kommunikation

- **Bygg förtroende:** Identifiera sårbara och kritiska målgrupper för verksamheten. Hantera medarbetare, varumärke och förtroende som skydds-objekt och stärk förtroendet både internt och externt.
- **Riskkommunikation:** Hur kan verksamheten förbättra sin risk-kommunikation. Det baserat på egen risk- och sårbarhetsanalys (RSA) och säkerhetsskyddsplan samt kompletterande underlag.

5 Övning & utbildning

- **Övningar:** Genomför regelbundet, både enklare och komplexa, övningar. Exempelvis simuleringsövningar kring hantering av att vara i centrum för en kampanj som "LVU-kampanjen".
- **Utbildning:** Ge kontinuerlig utbildning till personalen inom relevanta områden.
- **Red Team Testing:** Detta innebär att en grupp experter, både interna och externa, testar verksam-heten ur flera perspektiv.

10 Rekommendationer

COMBITECH

6 Hotunderättelser

- **Hotbildsanalys:** Identifiera potentiella hot och hotaktörer för er sektor / bransch i allmänhet och er organisation i synnerhet
- **Digitalt fotavtryck:** Säkerställ kapacitet att identifiera informations-läckage, såsom data-dumpar och typosquatting.
- **Löpande monitorering:** Bevakning av hur verksamheten omnämns online (inkl. dark web) för att snabbt kunna bemöta direkta hot, desinformation eller negativ ryktesspridning.
- **Analysförmåga:** Etablera och utveckla en förmåga för OSINT, IT-forensik och webbanalys.

7 Omvärldsanalys

- **Beslutsstöd:** Tilldela en funktion ansvar för att utreda, bevaka och analysera relevanta och prioriterade informations-behov och frågeställningar.
- **Underättelsecykeln:** Använd underättelsecykeln som grundmetod, för att strukturera er omvärlds-bevakning och för att säkerställa att ni samlar in och analyserar relevant information
- **GAP-analys:** Genomför en gap-analys av verksamhetens förmågor, inklusive mediamonitorering såsom "Social Listening". Identifiera metoder, rutiner och tekniska verktyg samt eventuella gap i förhållande till informationsbehoven.

8 Rapportering

- **Etablerade kanaler:** Säkerställ att olika målgrupper snabbt och enkelt kan rapportera om utmaningar, risker och hot. Från allmän ryktesspridning till hat liksom direkta hot mot verksamheten och dess anställda.
- Exempel på olika målgrupper: anställda, konsulter, leverantörer, uppdragsgivare, nyckelaktörer inom egen sektor liksom allmänhet och media.

9 Samverkan & samordning

- **Intern samverkan:** Säkerställ kontinuerligt samarbete mellan olika funktioner, exempelvis ledning, beredskap, säkerhet, kommunikation, HR, arbetsmiljö och IT för att hantera funktions-överskridande utmaningar, risker och hot.
- **Sektorssamverkan:** Upprätthåll kontinuerligt samarbete med beredskapsmyndigheter och huvudintressenter inom egen sektor / bransch för att hantera gemensamma utmaningar, risker och hot.

10 Syntetisk media

- **Initiera utbildning:** för alla anställda, om AI i allmänhet och syntetisk media i synnerhet.
- **Förbättrad autentisering:** Implementera robust analog / digital flerfaktors-autentisering för att skydda mot ”Deepfake-imitationer”.
- **Krisresponsramverk:** Etablera en kris-hanteringsstrategi för Deepfake-incidenter, inklusive snabb respons för att mildra riktad desinformation.

Omvärldsanalys och framsyn?!

COMBITECH

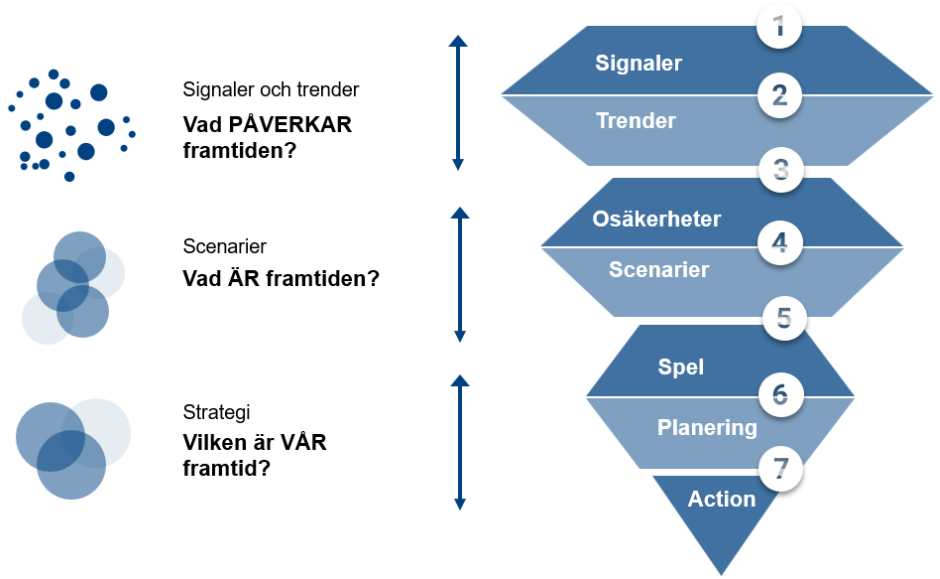
- **Omvärldsanalys** innebär en systematisk och kontinuerlig process på strategisk och operativ nivå avseende insamling, analys och kommunikation av omvärlds-information för att öka organisationens konkurrenskraft. Omvärldsanalys handlar om att noggrant bevaka och analysera förändringar för att förstå deras potentiella påverkan på organisationer, individer och samhället i stort.

- **Underättelsecykeln** är en beprövade metod för att systematiskt samla in, analysera och sprida information om en specifik omvärld. Metoden består av följande steg: 1) Planering/inriktning 2) Insamling 3) Bearbetning 4) Analys 5) Delgivning.

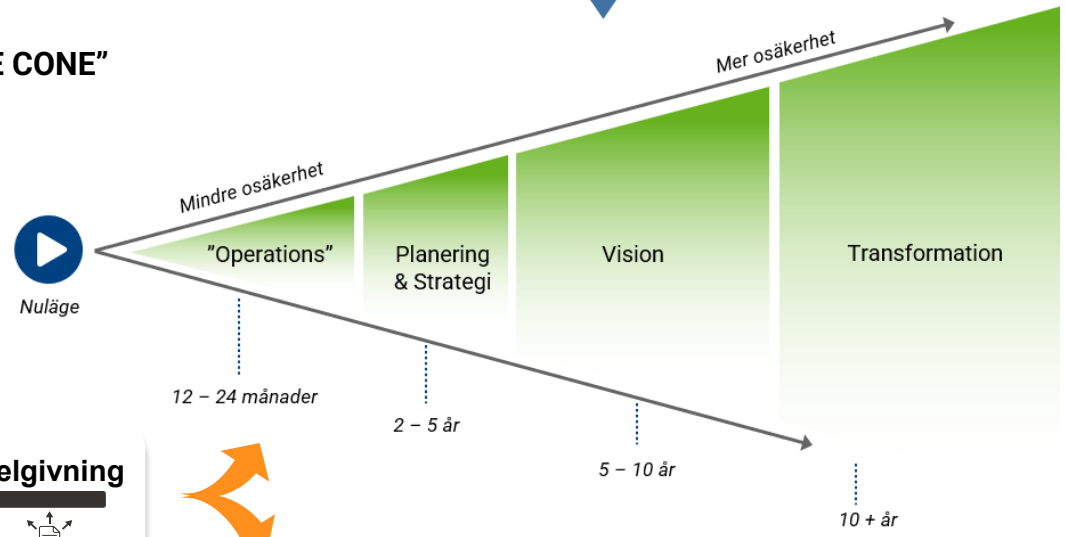
- **Framsyn och scenarioanalys** handlar om att systematiskt utforska möjliga framtida händelseutvecklingar. Exempelvis inom en viss avsatt tidsram eller ett specifikt område. Dessa metoder hjälper organisationer att både förutsäga och påverka framtida scenarier, samtidigt som de bygger en kultur av kontinuerligt lärande och anpassning. Genom att analysera olika scenarier får organisationer en djupare förståelse för de trender och osäkerheter som kan påverka deras framtid, vilket gör det möjligt att utveckla flexibla och robusta strategier och handlingsplaner för att hantera utmaningar och möjligheter.

- **Generativ AI** kan bidra till effektivisering och ökad kvalitet genom att automatisera insamling och bearbetning av stora mängder data. AI kan upptäcka dolda mönster och trender som annars skulle kunna förbli osynliga för mänskliga analytiker. Trots dessa framsteg är mänsklig bedömning fortfarande nödvändig för att tolka och värdera informationen korrekt, vilket innebär att AI bör ses som ett komplement till, snarare än en ersättning för, mänsklig expertis.

"SEVEN STEP FORECASTING FUNNEL"



"TIME CONE"



SYSTEMATISK OMVÄRLDSANLYS - UNDERÄTTELSECYKELN

Hur kommer vi igång?

COMBITECH

Data | Processer & metoder | Kompetens | Tillförlitlighet | Verktyg

Byggblock för systematisk omvärldsanalys

Tilldela ansvar

Etablera struktur, ex: underättelsecykeln

Fokus & prioritet

Övergripande
- Policy- ansvarsområde
- Bransch, intresseområden

Information
- Narrativ
- Huvudbudskap

Varumärke
- Förtroende
- Kärnvärden

Målgrupper
- Ledning & personal
- Partners & kunder
- ...

Tekniska verktyg

Media
- Press & mediabevakning

Social
- Stödja målgruppsanalys
- Social Listening

Integritet
- ”Brand Watch”
- Deep web/Darknet
  - Informationsläckage och ex. typosquatting.

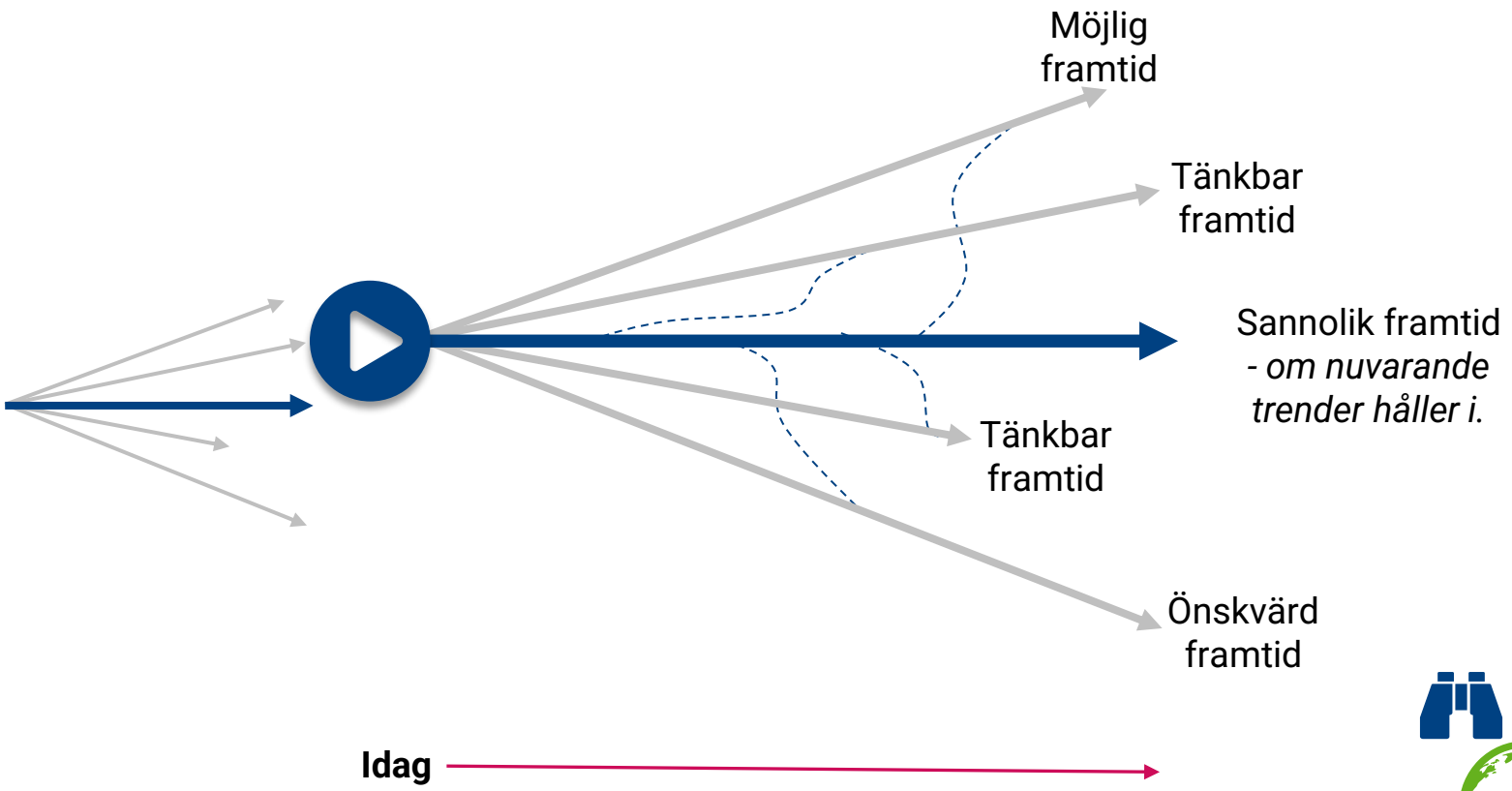
Fact-checking
- Stödja granskning & verifiering

Hot & sårbarheter

Bedöm egna sårbarheter, risker och hot:

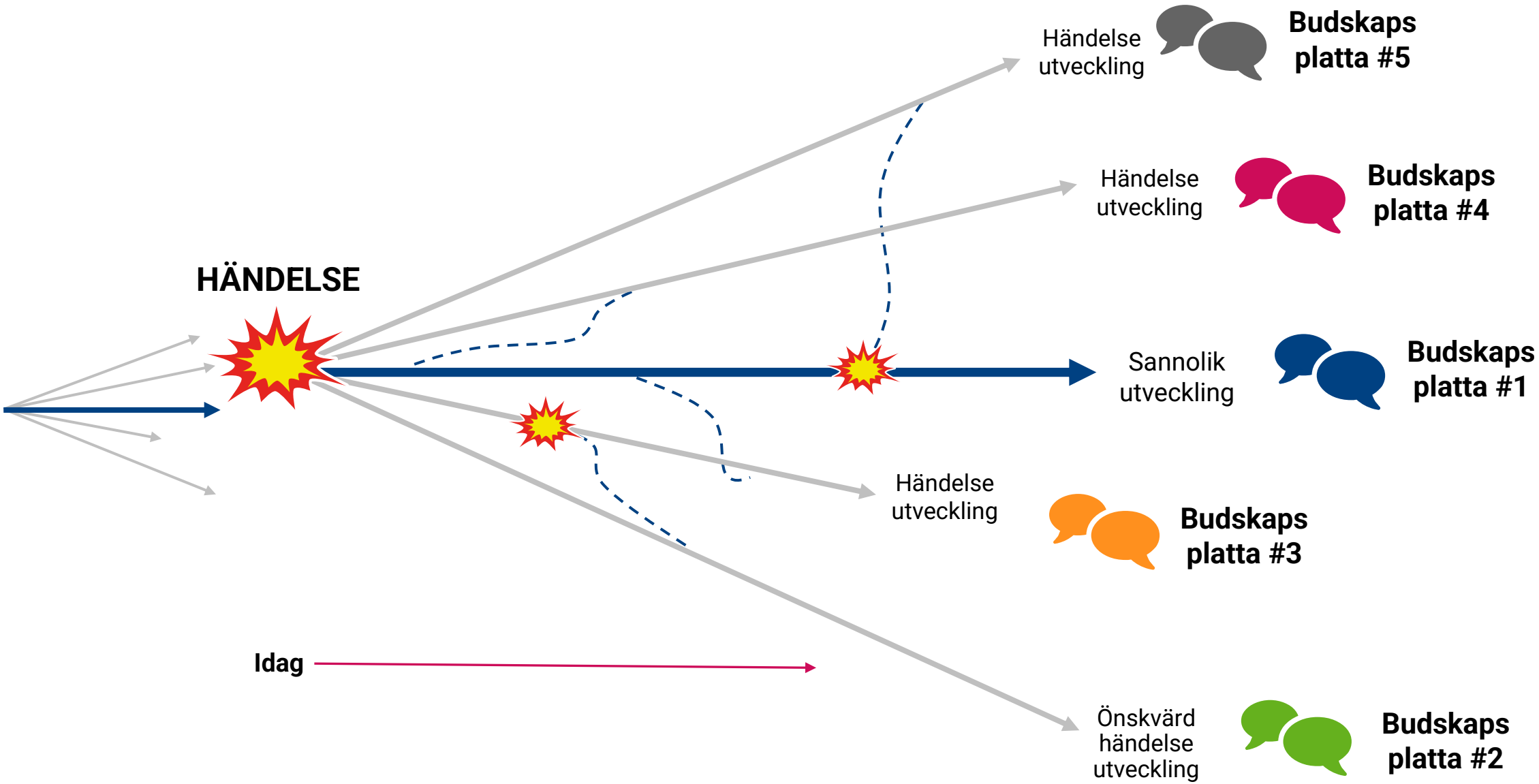
- Interna/externa sårbarheter
- Nätverk och aktörer
- Narrativ
- ”Värsta scenario”
- Red-teaming (spela djävulen)

… från signal till aktivitet



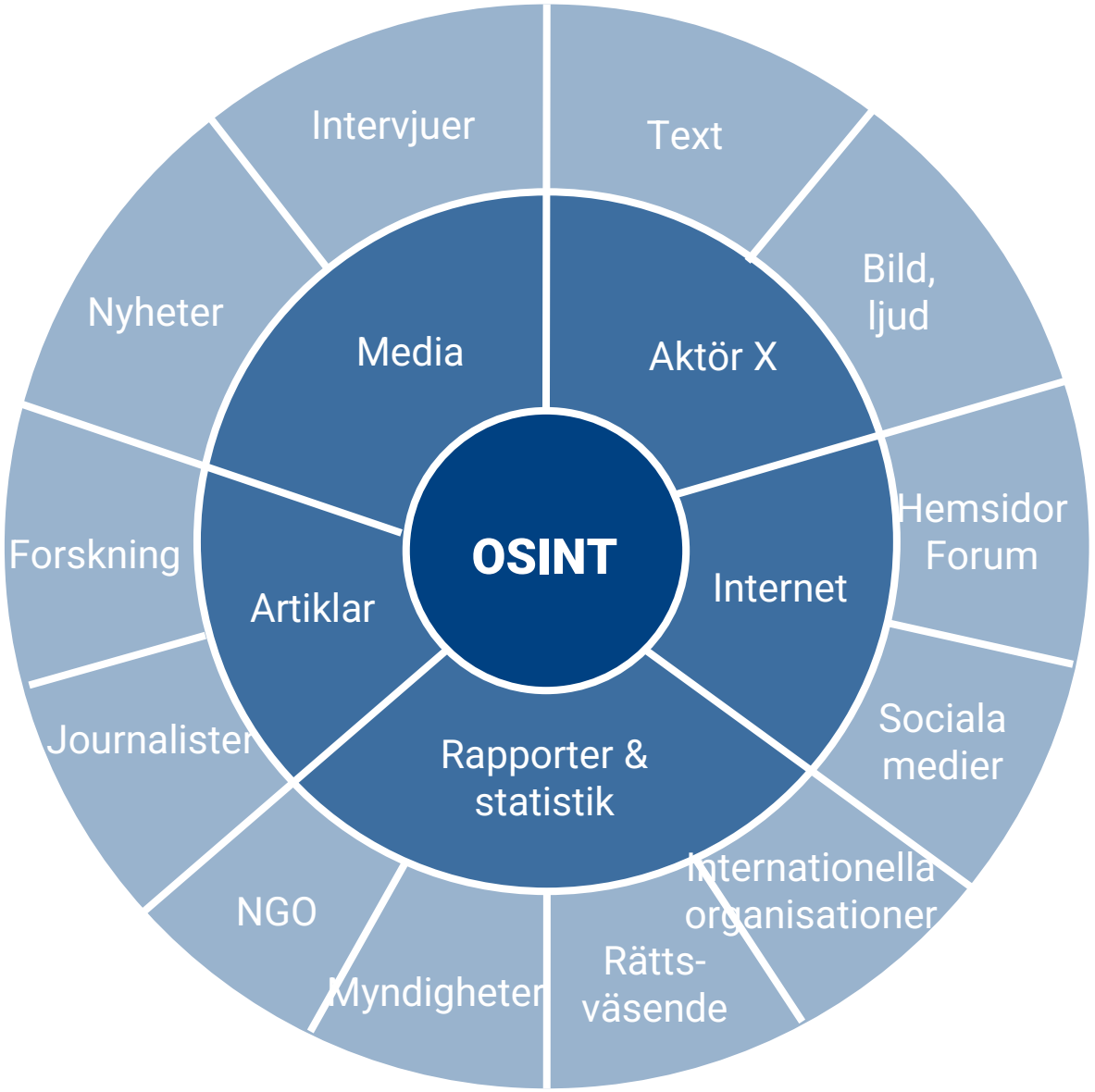
… händelsehantering

COMBITECH



Data | Processer & metoder | Kompetens | Tillförlitlighet | Verktyg

Byggblock för systematisk omvärldsanalys



COMBITECH

Exempel

Assistenter

ChatGPT · Gemini · perplexity · Copilot

Google Alerts

Google Alerts – still strong

Marknad & Kommunikation

sprinklr · Talkwalker · Meltwater · sproutsocial · Brandwatch · all ears

Risk & hotunderättelser

Recorded Future · Silobreaker · traversals

Informationspåverkan

storyzy · BLACKBIRD.AI

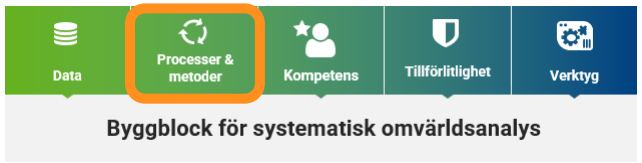
Mångsidiga

dcipher analytics · TBox

Detektivarbete

Bellingcat's Online Investigation Toolkit

Rapportera – 8 frågor



COMBITECH

Kort beskrivning av händelse och informationen

1. Hur upptäcktes händelsen? I vilka forum/media?
2. Misstänker ni att det har koppling till en illasinnad aktör?
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?

Standardisera
(ex. incidentrapport)

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
- Mediemedveten - Mediemyndigheten
- 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:

Mediemedveten - Mediemyndigheten

Våra favoriter:

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)

- PSYCHOLOGICAL DEFENCE AND INFORMATION INFLUENCE – A TEXTBOOK ON THEORY AND PRACTICE | myndigheten för psykologiskt försvar
- Att möta informationspåverkan – Handbok för journalister (mpf.se)
- Bli inte lurad - Handbok för privatpersoner | Myndigheten för psykologiskt försvar
- Historien som slagfält: Rysslands påverkanskampanj mot Finland 2025 | Myndigheten för psykologiskt försvar
- 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 3: Building resilience to information threats

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
- Digitala lektioner | En öppen lärarresurs

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 och 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

Mitt digitala fotavtryck

Roller och intressen

Privat och på jobbet. Vilka behörigheter och tillstånd har jag? Digitala och fysiska. Vilka behörigheter och tillstånd har jag delat ut till andra?

Intressen, hobbys – djur, idrott, kultur, resa, friluftsliv osv.

Medlemskap

Medlemskap, lojalitets-program, abonnemang, streamingtjänster, familjemedlemmars abonnemang.

”Spela djävulen”

– hur kan den här informationen användas för att påverka dig?

Min egen berättelse

Vad delar jag i olika nätverk. Vilka beteenden har jag? Profil på Facebook, Instagram, Linkedin mm. status-uppdateringar, incheckningar.

”Googla” dig själv”

Informationsläckage

[Är min mejladress säker? (sakerhetskollen.se)]

Andras berättelse

Vad delar vänner och familj om mig? Vad delar din kollega, dotter, granne…?
I vilka sammanhang och miljöer dyker jag upp? Bilder, album, inlägg, status-uppdateringar, incheckningar …

”Osynliga spår”

Positionsdata – karttjänster, appar. Stänger jag av Wifi, Bluetooth? Mobildata, Smarta prylar.

COMBITECH

Våra tjänster

Exempel på tjänster

- Föreläsningar och rådgivning
- Utbildningar (allmänna, fördjupningar)
- Övningar, spel och workshops
- Omvärldsanalys och utredning (ex. exponeringsanalys, hotbildsanalys).
- Risk och säkerhetsskyddsarbete (inkl. säkerhetskultur)
- Strategiarbete, scenarioanalys och framsyn
- Proaktiv kommunikation (ex. risk-kommunikation, försvarsvilja).
- Utvärderingar (ex. Stresstest, gapanalys, mognadsbedömning)

Operativt stöd,
(ex. incidenthantering & kriskommunikation)

Verksamhetsanpassade filmer

Table-top och simuleringsövningar

Utredningar och omvärldsbevakning

Med utgångspunkt i er verksamhet

COMBITECH

Shaping a smart and resilient society