Juridik i den Digitala Tidsåldern -

AI, Cybersäkerhet & ny Lagstiftning

Charlotta Kronblad

START kl 9.00

- Presentationer: vem jag är – vem ni är. Mål och förväntningar

Juridik, digital teknologi – och algoritmisk (o)rättvisa

- FIKAPAUS 10:30
- Integrerade övningar och diskussioner

LUNCHPAUS 12-13

Cybersäkerhet och ny lagstiftning:

- AI Förordningen, NIS2, CRA, GDPR
- FIKAPAUS 14.30
- Integrerade övningar och diskussioner

AVSLUTNING 16.00

- Nya insikter och fördjupad förståelse för de juridiska utmaningarna i en digitaliserad värld
- Förstå hur (och varför) den digitala transformationen ställer nya krav på rättssystemet
- Dela era erfarenheter och praktisk kunskap: hur kan vi skapa värde från juridiken, och hur kan domare och andra jurister involveras på vettigt sätt
- Överblick av ny och relevant lagstiftning

Charlotta Kronblad

GÖTEBORGS UNIVERSITET
HANDELSHÖGSKOLAN

ADVOKATBYRÅ

STOCKHOLM SCHOOL OF ECONOMICS
HOUSE OF INNOVATION

MANNHEIMER SWARTLING

UDDEVALLA TINGSRÄTT
SVERIGES DOMSTOLAR

VOLVO
Volvo Group

GÖTEBORGS UNIVERSITET

Digital Transformation of the Legal Field - A Bubble in Trouble

Doktorsavhandling, 2021

Digital Transformation | Digitalization | Legal Tech | Professional Service Firms | Law Firms | Institutional Complexity | Institutional Logics

Examination
2021-08-20 13:15 -- 00:00
Zoomlink Password: 132654
Opponent: Elena Raviola, University of Gothenburg

Online disputation

Läs hela texten (PDF)

Era förväntningar på dagen

- Bli entusiasmerad och inspirerad
- Lära mer – För med mer kunskap kanske vi vågar agera
- Få konkreta tips: hur använder advokater AI? Hur används det på våra domstolar?
- Framtidsspana
- Se nya affärsmöjligheter
- Titta på ny lagstiftning (ex AI förordningen), vilka möjligheter den kan bidra till

universitet
Uppsala unive...

Nabo
Juridik - Nabo

Juridik
Vad är juridik | Juridik

Juridik och etik i den nya tiden?

- Förändrar teknologin förutsättnignar för rättvisa
- Hur påverkar det våra domstolar och rollen, och arbetet, som domare

DIGITAL

TRANSFORMATION

AI

SMART?

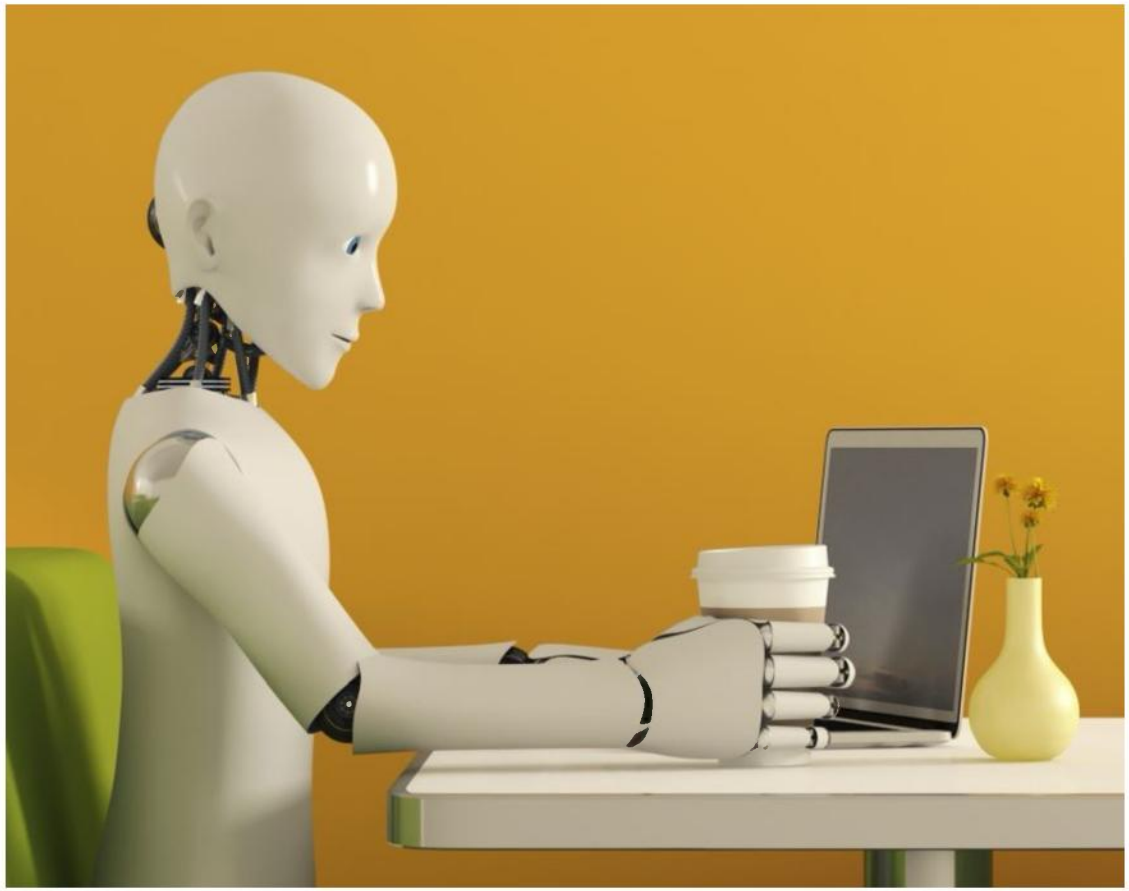
Input Manipulation Attacks in the Wild

AI SWEDEN

2019

Black tape added to 35 mph speed limit sign tricks self-driving car to 85 mph

https://www.technologyreview.com/2019/03/25/1216/emtech-digital-dawn-song-adversarial-machine-learning/



Riksarkivet Swedish National Archives
4 278 följare
2 v •

+ Följ

Riksarkivet söker dig som vill leda, utveckla och stärka vårt arbete inom forskning och kunskapsspridning. Du får leda en dynamisk avdelning på 30 medarbetare och driva viktiga initiativ, inklusive digitalisering och ... mer

Peter Krantz och 2 till

2 inlägg som lagts upp igen

Gilla Kommentera Omdela Skicka

GENERATIV
AI

Diskussion: Hur arbetar ni med AI idag och hur fångar ni upp möjligheter och risker?

Våga testa! Och lär dig prompta – för prompten ger svaret (generativ AI)!

Positiv användning av Legora (tidigare Leya) samt Qura och Copilot, bra användning också av Juno, Harvey och Lexnova

AI verktyg används för rättsutredningar, analys, och för att transkribera, översätta och sammanfatta material

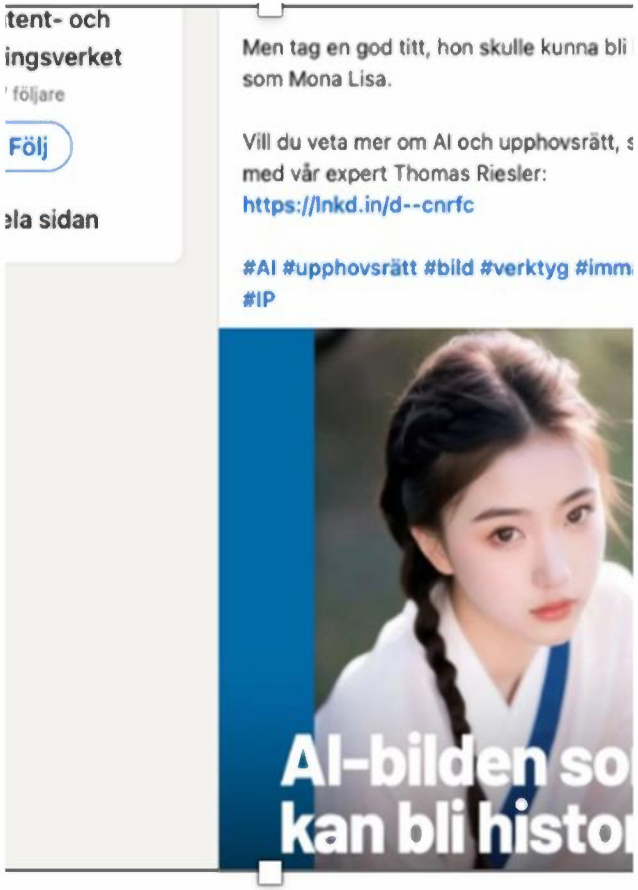
AI verktygen skapar effektivitet och bättre träffsäkerhet, samt kan vidga vyer och ge arbetet en viss rikttning (kan användas för att skapa neutrala och köp/sälj vänliga versioner av avta.)

Men, se till att ifrågasätt det som AI skapar/genererar. Ta resultatet med en nypa salt. Dubbelkolla och ifrågasätt.

Vilken träningsdata som används är viktig, liksom vilken språkmodell (LLM) som används.

JURIDIK I FRAMTIDEN

NYA
RÄTTSFRÅGOR



Annika Nordenskiold prisas för sina AI-bilder: ”En magisk konstform”

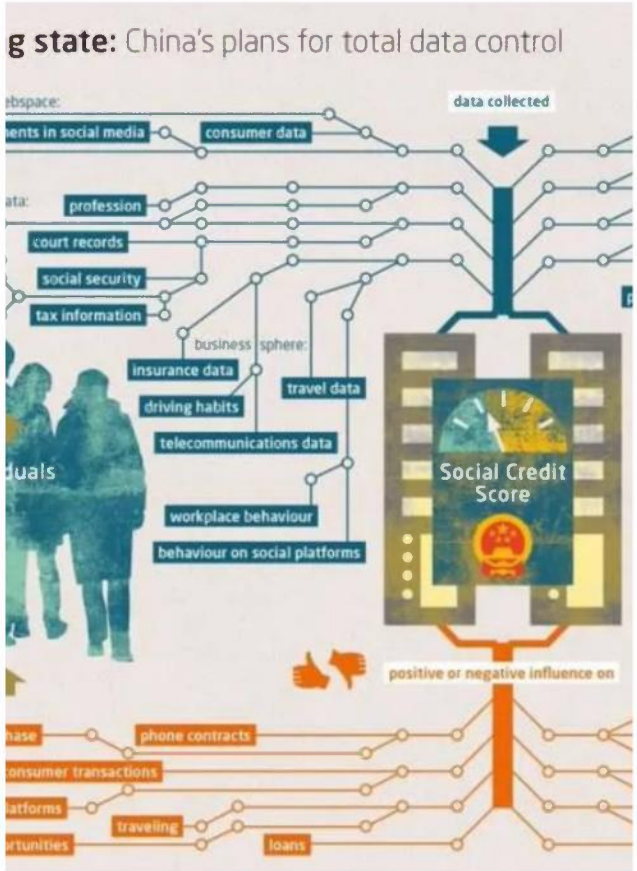
Publicerad 2023-10-17

MOBILITET

Människa eller maskin – vem bär ansvaret när olyckan är framme?

Storbritannien har satt ner foten i frågan vem som bä ansvaret när självkörande fordon är inblandade i olyckor. I landets nya färdplan för autonoma fordon slår regeringen fast att mänskliga förare aldrig bär ansvaret om en dator framför bilen – det gör tillverkaren.

NYA
MÖJLIGHETER
ATT STYRA
SAMHÄLLEN



NYA
BEVISFRÅGOR

Donald Trump i svensk kortfilm -

EDITORS AND LIBRARIANS: KILL FROM YOUR SYSTEMS AND ARCHIVES PHOTO LB1110, SLUGGED BRITAIN ROYALS AND TRANSMITTED ON SUNDAY, MARCH 10, 2024. AT CLOSER INSPECTION IT APPEARS THAT THE SOURCE HAS MANIPULATED THE IMAGE. NO REPLACEMENT PHOTO WILL BE SENT. - This undated photo issued on Sunday March 10, 2024 by Kensington Palace shows Kate, Princess of Wales with her children, Prince Louis, left, Prince George and Princess Charlotte, taken in Windsor, England, by Prince William earlier this week. The Princess of Wales shared a message on social media thanking the public for their continued support and wishing people a Happy Mother's Day. (Prince of Wales/Kensington Palace via AP)

Diskussion: Fundera på uttrycket “etisk AI” finns det? Vad innebär en ansvarsfull användning av AI?

Etik ja – men vems etik? Vem har makten bakom? Vad händer när etiken ändras? Etik är föränderligt…

- ex USA förändrad lagstiftning om aborter - plötsligt används digitala spåt *fem-tech* appar (preventivmedel) för att bevisa att kvinnor varit gravida/ gjort abort.. Samma för gay-dating-appar som används i repressiva samhällen för att bevisa olagliga homosexuella handlingar

Det handlar inte om Etisk AI utan om etisk **användning** av AI

Kan en etisk certifiering av användningen vara en lösning.

Det pågår en diskussion inom advokatsamfundet om dessa frågor, men AI är svårkontrollerat och utvecklas snabbt. Och vi har dessutom ett digitalt beroende av USA att ta hänsyn till

ALGORITMER

We are “*stumbling zombie like into digital welfare dystopia*” - Phillip Alston

UN Report/ 2021

Skolplaceringskatastrofen 2020

- I Göteborg placeras 12000 varje år (till 0, 4 och 7)
- Grundskoleförvaltning använde 2020 - för första gången en digital mjukvara
- För "ökad effektivitet" och "likabehandling"
- Systemet instruerades att placera barnen på "närmsta" skola, och när den var full, på annan "närliggande" skola.
- Men… algoritmen visste inte om älven
- Barn placerades långt bort, med domino-effekter i 6 led, vilket orsakade runt 1400 "felplacerade" barn

ALGORITMISK (O)RÄTTVISA

Rättsäkerhet i en digital kontext

- Min forskning visar att rättssäkerheten haltar – mycket på grund av att den juridiska infrastrukturen och processrätten inte har uppdaterats för digitalisering
- Vi kan endast överklaga individuella beslut, inte laglighetspröva kod, bevisbörda placeras på den sökande även när motparten kontrollerar bevisningen

Svenska Dagbladet Nyheter Näringsliv Kultur Ledare Debatt

Jo Hamilton och Alan Bates drabbades båda av skandalen med brittiska postkontoren. Foto: Belinda Jiao/Reuters, Mega

Ett felaktigt datasystem innebar att hundratals oskyldiga personer dömdes. Det har kallats den största rättsskandalen i brittisk historia. På nyårsdagen sändes första avsnittet i en tv-serie om fallet – sedan förändrades allt.

BBC Sign in Home News Sport Earth Ree

SOUNDS Home Music Podcasts My Sounds

The Great Post Office Trial

The extraordinary story of a decade-long battle with the Post Office, fought by their own sul postmasters. Some call it the widest miscarriage of justice in UK legal history.

EPISODES (21 AVAILABLE)

Introducing The Great Post Office Trial

The extraordinary story of a campaign to uncover a massive scandal at the Post Office.

3 mins | 24 May 2020

POLITICO

HOT TOPICS WAR I

Charlotta Buxton
Publicerad 2024-01-20

Följ skribent

Dutch scandal serves as a warning for Europe over risks of using algorithms

The Dutch tax authority ruined thousands of lives after using an algorithm to spot suspected benefits fraud – and critics say there is little stopping it from happening again.

Most Read Articles

1. Finnish leaders announce backing for NATO membership
MAY 12, 2022 | 9:09 AM

2. UK economy shrunk in March as service industry struggles
MAY 12, 2022 | 8:44 AM

#NotMyDebt

confused & concerned about your Centrelink debt?

Home The issue Stories Help! Get Involved Senate Inquiry About

You are not alone.

You should lodge a dispute or get legal advice if you think your debt is in error.

Share your story with us

Read other stories

#NotMyDebt Shared Stories

Försäkringskassans fuskjagande AI

Hemlig AI såg oskyldiga kvinnor som vab-fuskare

DAGENS NYHETER. Nyheter Sverige Världen Ekonomi Kultur

05:53 Dela

Brittiskt dataprogram ska förutse mord

Den brittiska regeringen håller på att utveckla ett hemligt dataprogram för att göra ”mordprognoser” på enskilda individer, rapporterar The Guardian. Programmet kallades ursprungligen för ”homicide prediction project”, men namnet har ändrats till ”sharing data to improve risk assessment”.

Dess existens avslöjades av den fristående organisationen Statewatch, som granskar statlig verksamhet som kan hota medborgerliga friheter.

– Justitiedepartementets försök att bygga detta system för att förutse mord är det senaste skrämmande och dystopiska exemplet på regeringens avsikt att utveckla så kallade system för att ”förutse” brott,

säger Sofia Lyall, forskare knuten till Statewatch till Guardian.

Justitiedepartementet hävdar att programmet enbart ska användas för forskning.

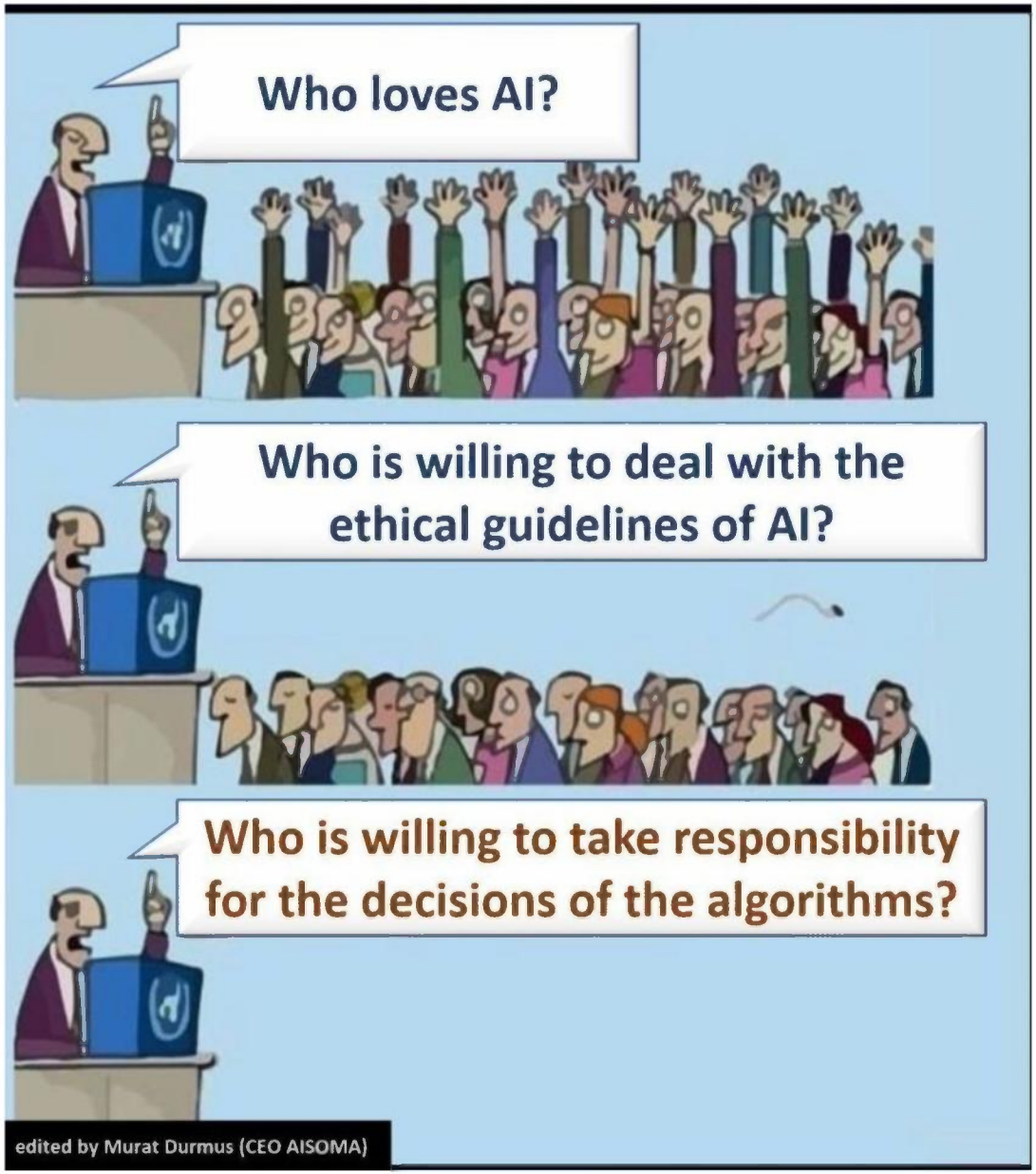
Ulrika By

Är detta juridiskt korrekt? Är det etiskt?

- Minorityreport på riktigt
- Vad hände med oskyldighets presumptionen
- https://www.theguardian.com/uk-news/2025/apr/08/uk-creating-prediction-tool-to-identify-people-most-likely-to-kill

LÄSTIPS


AI & MAKTEN ÖVER BESLUTEN
MAJA FJAESTAD, SIMON VINGE (RED.)
Vad alla borde veta om algoritmer i offentlig sektor


Who loves AI?
Who is willing to deal with the ethical guidelines of AI?
Who is willing to take responsibility for the decisions of the algorithms?
edited by Murat Durmus (CEO AISOMA)

LUNCH

Återsamling kl 13

Cybersäkerhet och ny lagstiftning
Diskussion: Vad är cybersäkerhet?

Att skydda sig mot cyberangrepp

Att vara medveten om risker

Att ha tydliga regler och en säkerhetskultur

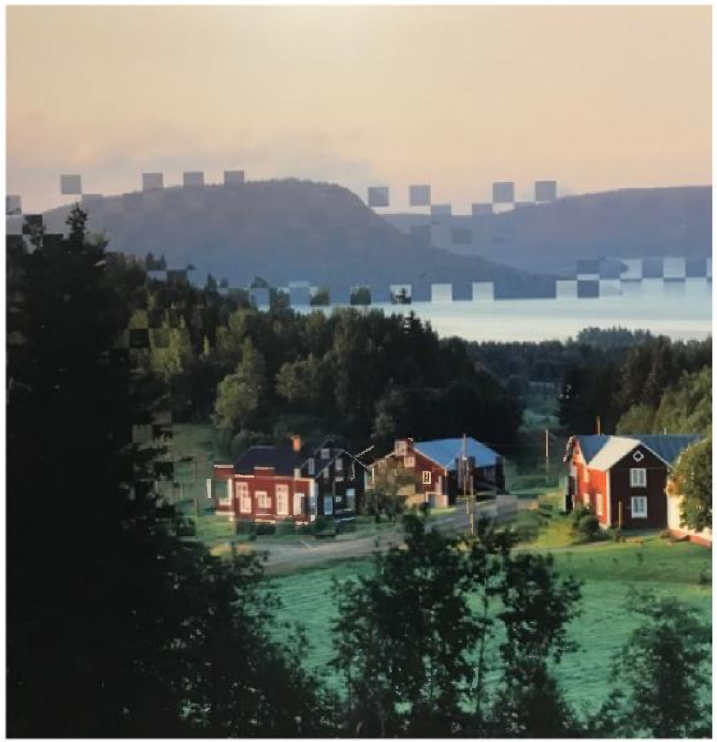
Det går att testa säkerhet och mognad genom “bluffmail”

Det är viktigt att information inte bara skyddas utan att den också är tillgänglig vid behov, och att den stämmer

En ny dimension för information & kommunikation

Cybersäkerhet - definitioner

- *"Measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack"* Confident Cybersecurity - Jessica Barker
- *"Cybersäkerhet = säkerhet relaterad till internet ex skydd mot skadlig kod. En allt mer kritisk funktion pga samhällets digitalisering"* GUs kurs i informationssäkerhet –(för att visa vad kursen inte handlar om)
- *"The world's interconnectedness means that cybersecurity is not just about protecting information; it's about safeguarding our way of life." Mastering Cybersecurity – Jason Edwards*



Människan står i centrum

- Vi skyddar ultimat systemen för att skydda oss: våra jobb, våra finanser, vår identitet och fysisk säkerhet.
- Det är personer som; designar, skapar, testar, använder, missbrukar och förstör teknologi, hård och mjuk-vara, och informationssystem
- "*There is no such thing as a malicious machine – it is all about the people and the human element*" Jessica Barker (2024)

”digital security always has a physical dimension”

- Internet bygger på en fysisk infrastruktur
- Nätverk av sammankopplade system står i server hallar – som behöver kylas (Norrland bra placering – billig grön el och gratis kylning)
- Information färdas via koppar ledningar eller glas fiber optik– där laserstrålar sänder information med ljusets hastighet - Kablar under haven. Ofta placerar center nära dessa ex i Groningen i Nederländerna - där transatlantiska kabeln slutar
- Fysisk placering av center och hallar beror också på jurisdiktion, vill komma åt viss reglering

- Cyberangrepp sker dagligen mot Sverige och de blir alltmer avancerade. Metoder och verktyg för cyberangrepp utvecklas ständigt och hotaktörernas förutsättningar förändras i takt med teknikutvecklingen

- Samtidigt har digitalisering, globalisering och den snabba teknikutvecklingen gjort samhället mer sårbart.

- Hoten handlar om underrättelsehot från främmande makt; och från kriminella som utsätter verksamheter för brott.

- Det kan ske genom exempelvis lösenordsattacker, e-postangrepp, nätfiske, skadlig kod eller angrepp mot mobila enheter.

Cybersäkerhet

Cyberförmåga och möjlighet att verka i den digitala miljön är avgörande inom Säkerhetspolisens samtliga verksamhetsområden.

Vad är informationssäkerhet?

- Informationssäkerhet handlar om att skydda information som kan vara i olika former - Text, ljud, bilder och film
- Omfattar all information oavsett hur den lagras, bearbetas och kommuniceras
- Informationen kan hanteras med stöd av IT, lagras i pappersform eller direkt av oss människor (i form av tal)

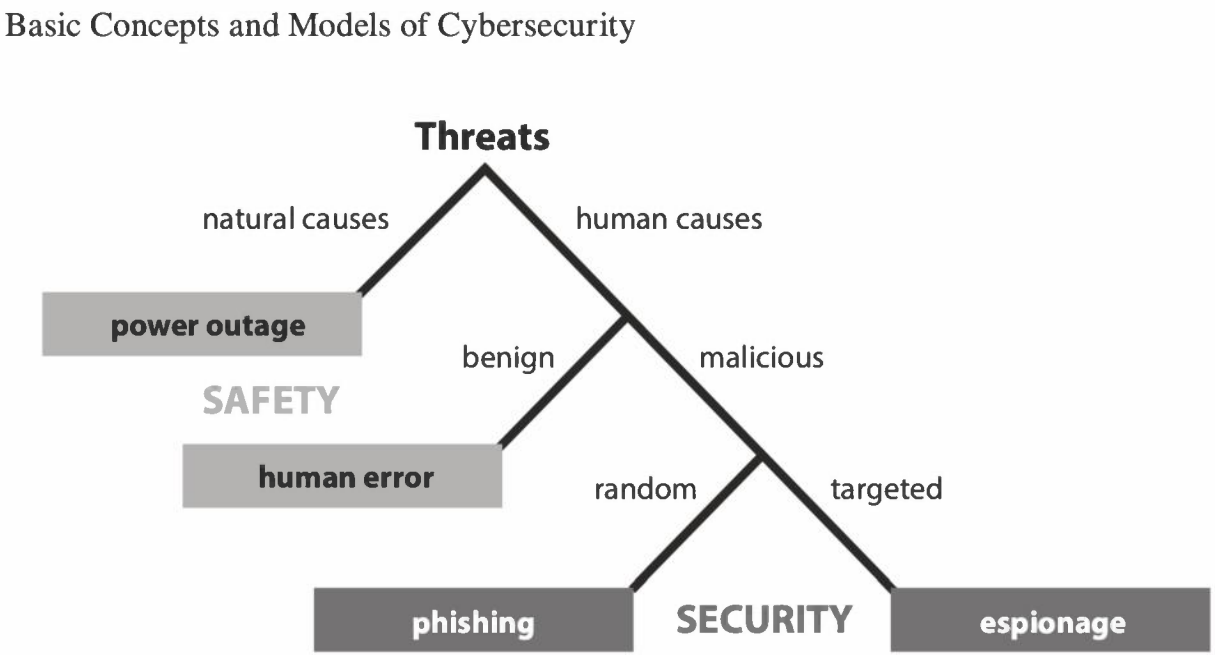
- *Konfidentialitet* att informationen inte tillgängliggörs eller avslöjas för obehöriga
- *Riktighet*: att informationen är fullständig och korrekt
- *Tillgänglighet*: att informationen är åtkomlig och användbar om den begärs av ett behörigt objekt

Centrala begrepp på engelska

- Confidentiality: prevent unauthorised information gain.
- Integrity: prevent or detect unauthorised modification of data.
- Availability: prevent unauthorised deletion or disruption.

Skillnad på *safety & security*

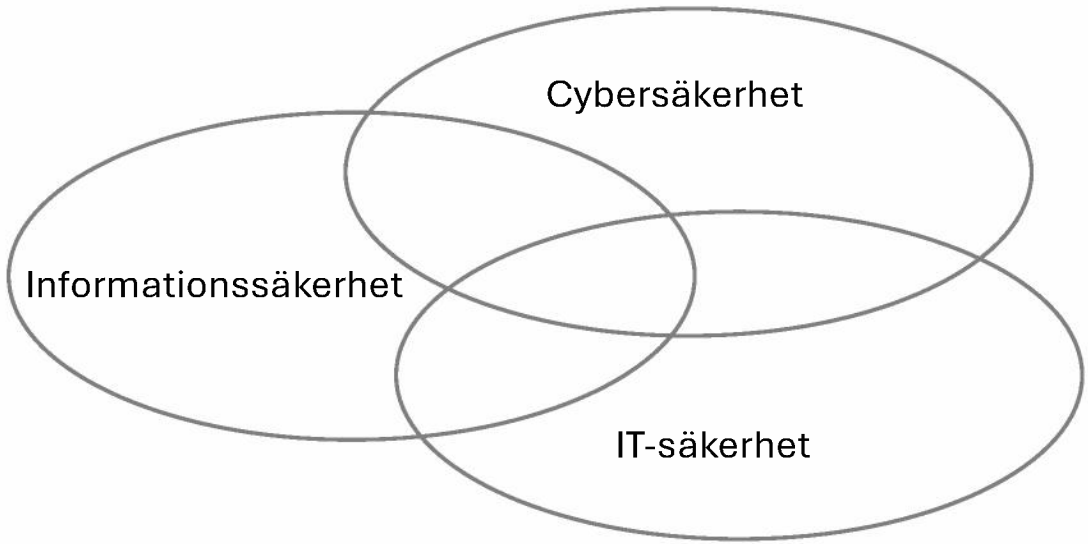
- Herrmann & Pridöhl, (2020) *The ethics of cybersecurity* Springer



Vad är IT-säkerhet?

- Fokuserar på den tekniska säkerheten, målet är att hålla systemen igång – upprätthålla IT säkerhet
- Säkerhet inom IT-system och IT infrastruktur
- Hit hör tekniska förutsättningar för säker informations lagring och spridning- kommunikation, kablar, ledningar, serverhallar, hårdvara, datorer. Hantering av diskar, USBstickor etc.

Begreppen relaterar och överlappar

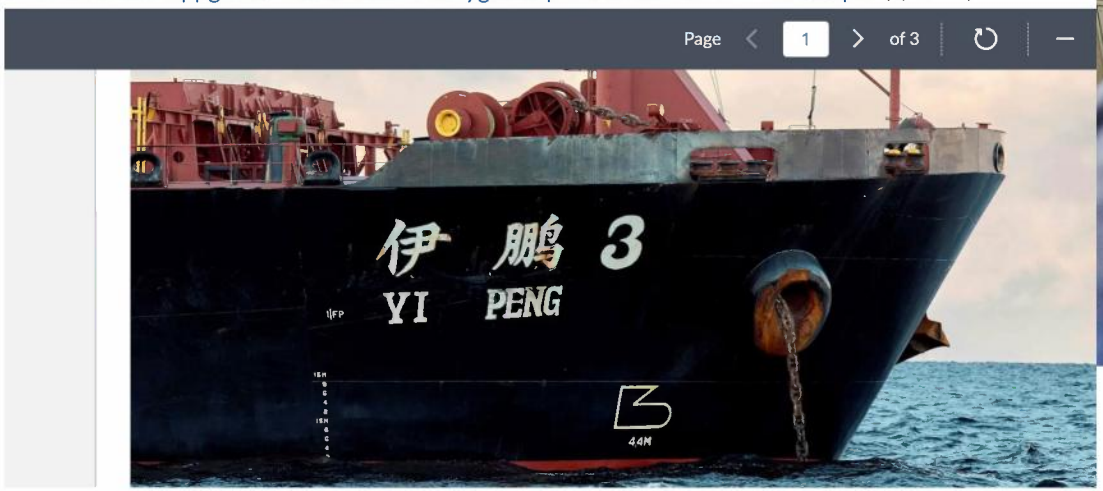


Övning: Analysera nyheter ur ett cyberperspektiv

- Vad handlar nyheterna om, var skulle du mappa in den: gäller det cyber-, informations- eller IT-säkerhets problematik?

DN Uppgifter: Det kinesiska fartyget släpade ankar i 16 mil - DN.se.

ownload 6 DN Uppgifter: Det kinesiska fartyget släpade ankar i 16 mil - DN.se.pdf (1,85 MB)



DAGENS NYHETER. Nyheter Sverige Världen Ekonomi Kultur Sport Klimatet Ledare DN

EKONOMI

De hackar värmepumpar och batterier till vardags: ”Det är ofta väldigt lätt”

Uppdaterad 2025-04-28 Publicerad 2025-04-28

DAGENS NYHETER.

SVERIGE

Hemliga angreppet mot Sverige under koranbränningarna

Uppdaterad 2024-09-24 Publicerad 2024-09-24

DAGENS NYHETER.

SVERIGE

KTH vill sparka professor – arbetade i Ryssland: ”Jag är inget säkerhetsproblem”

Uppdaterad 2025-03-18 Publicerad 2025-03-18

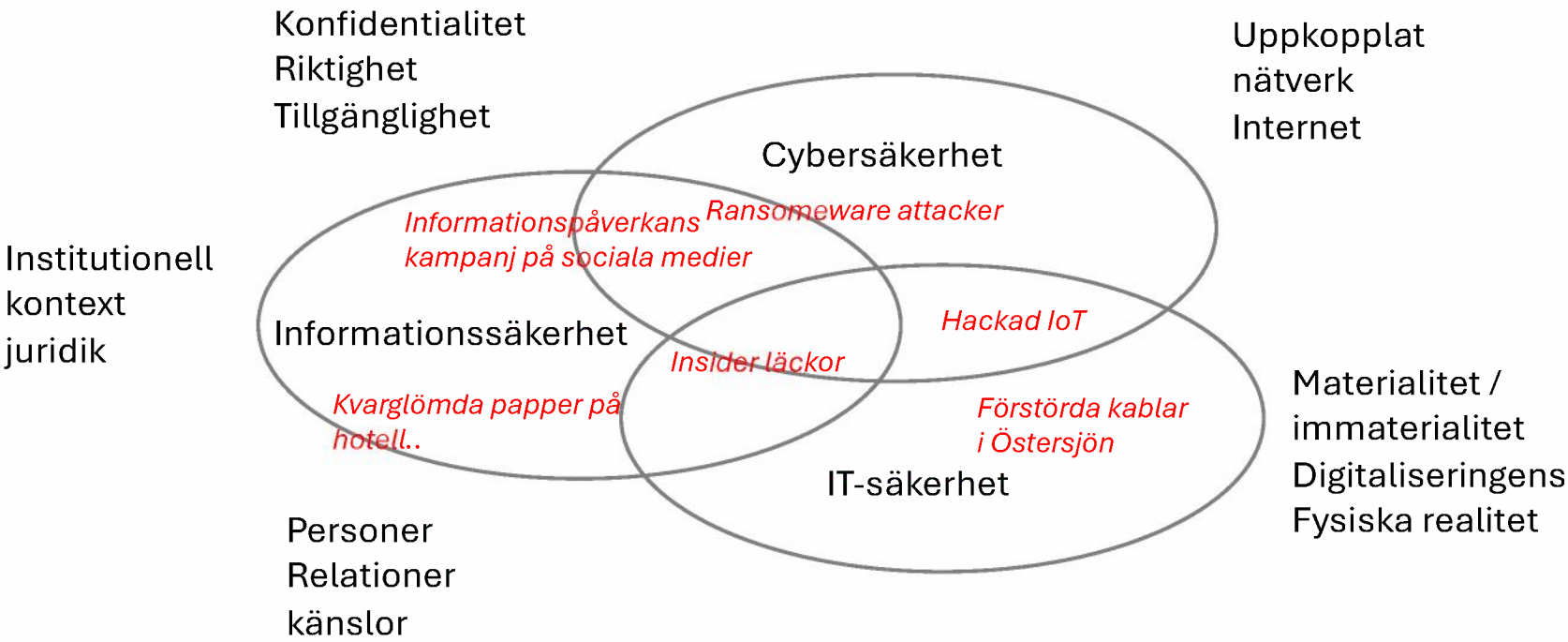
GENS NYHETER. Nyheter Sverige Världen Ekonomi Kultur

SVERIGE

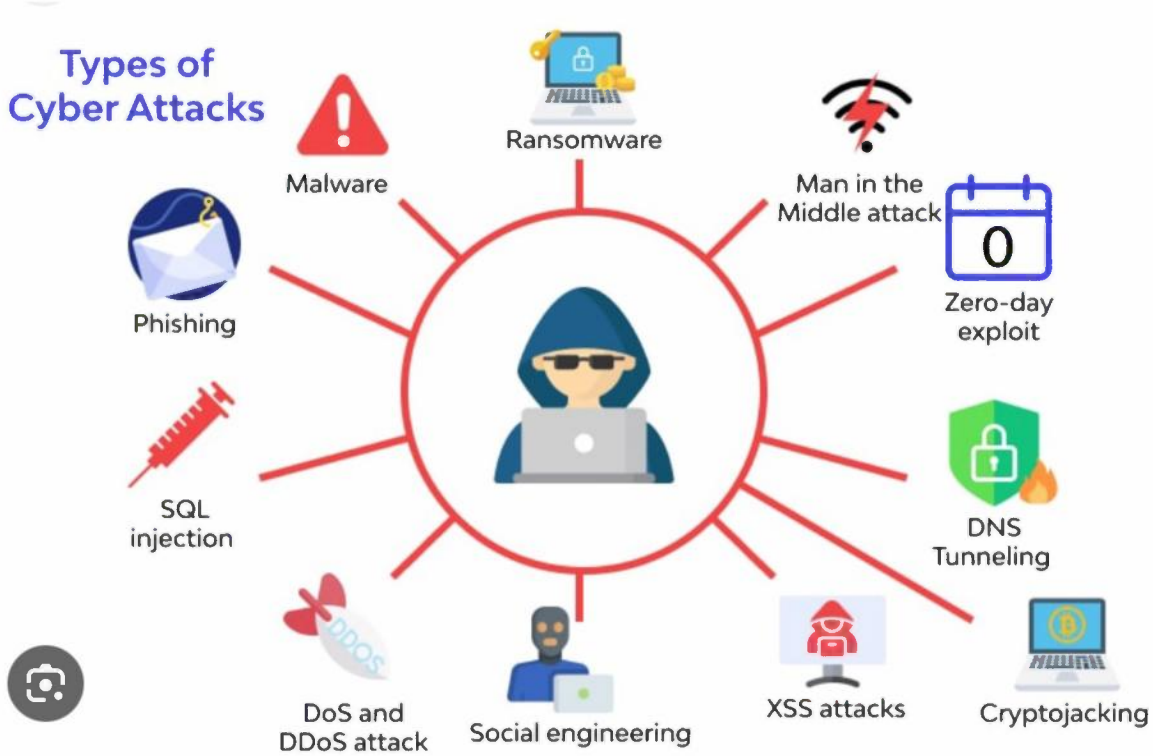
Städerskan som hittade Landerholms handling förhörts

Uppdaterad 2025-03-19 Publicerad 2025-03-19

Concept mapping



Begrepp inom cybersäkerhet

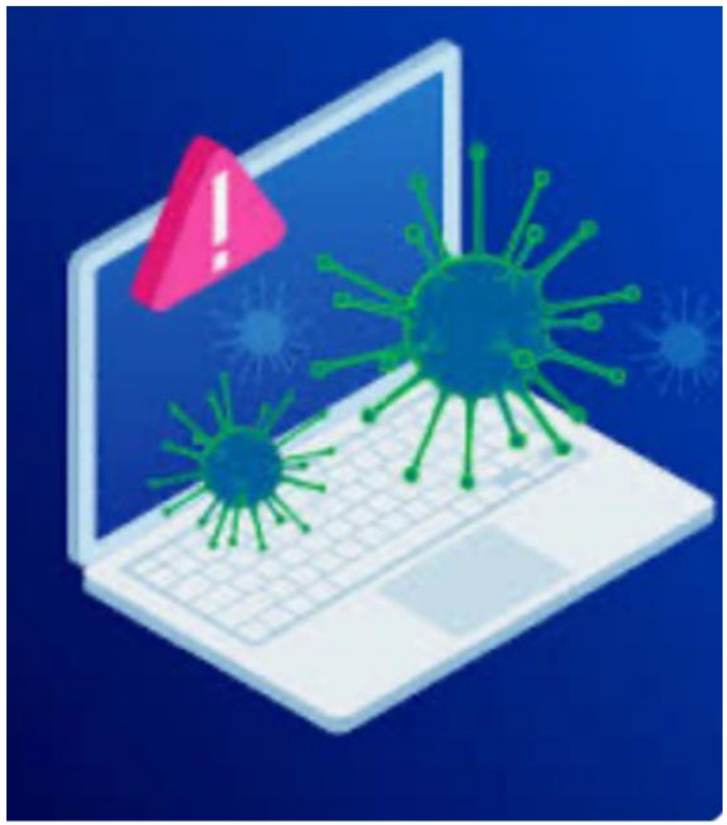


Malware (malicious software)

Skadlig programkod – för att skada din enhet /system, förstöra filer eller stjäla information.

Kan vara virus, trojaner, spionprogram

Från hobby-hackande och self replicating worms (för att undersöka Internets räckvidd) till big business



Ransomware attacks

Att begära lösen för att göra/ inte göra något - har blivit big business – ransomware as a service

Exempel från Sverige 2024 – Systembolaget – orsakade leveransproblem och tomma hyllor,

Tietoevry orsakade stora problem i myndigheter/kommuners system för HR löner, olika register etc

Ofta begärs lösen i kryptovalutor – 99% av fallen i Bitcoin. Forskning har visat att Bitcoins värde korrelerar mot ransomware-attacker (Barker, 2024)

“Everyone has to admit that without crypto, it would be a lot more challenging for ransomware and crime. Ever since Capone or earlier, the way governments have tried to fight organized crime is by putting regulations and responsibilities on the banks. Crypto offers a way through that for cyber criminals, even more so when they avoid regulated exchanges”

Benedict Hamilton, investigator of cybercrime,

in Hacked by Jessica Barker (2024)

“Chain hopping”
“Mixers”

Phishing attack

Försök att stjäla information – ofta genom synes legitima email och länkar (ser ut som det kommer från din bank, myndigheter) Skickas ofta till stort antal – hoppas någon svarar – ex. klickar på bifogad länk.

Använder sig av **social engineering** – skapa känsla av hot, stress – handla snabbt och utan eftertanke – men kan också använda sig av *flattering* och *authority bias*

Allt oftare med “**pretexting**” ett förberett trovärdigt narrativ

“**Spear phishing**” – riktat – individualiserat meddelande med namn, kanske barnens skola, familjemedlem etc- för att öka trovärdighet

“**Phone-spoofing**” när ett caller-ID gör att du tror källan är legitim (ex myndighet eller IT-support)

Difference Between Phishing, Vishing and Smishing

QR code-phishing

FBI varnat för stark ökning (2022) i **“Quishing”**

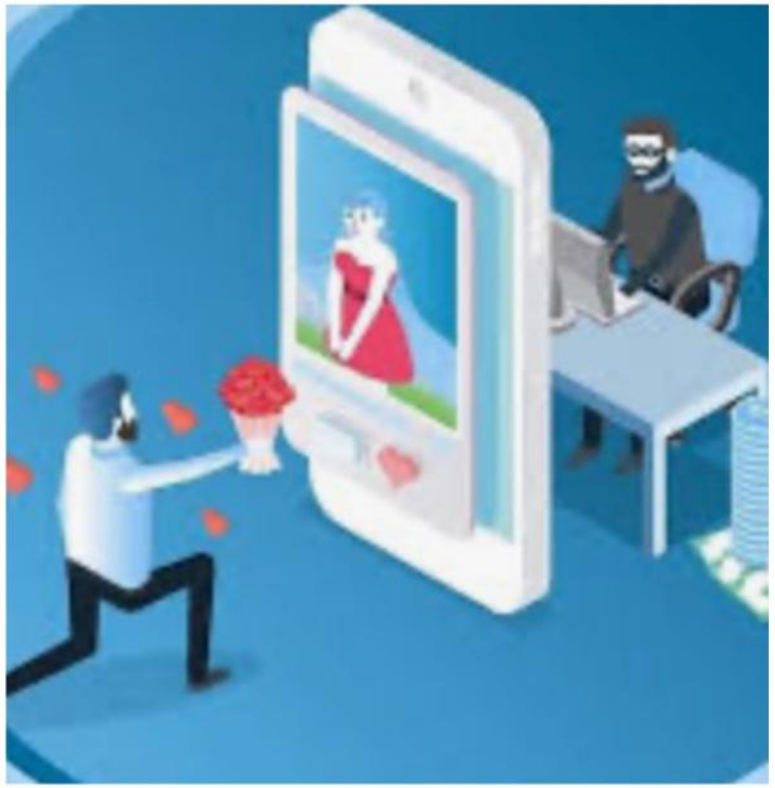
Ex. Kvinna scannade kod utanför bubbletea restaurang – lurad av erbjudande om gratis dryck för att fylla i en kort undersölning – men när hon scannade bilden laddades en ondsint app ner på mobilen som stal 20 000 dollar från hennes Internetbank

Romance Fraud / Bedrägerier

En fejkad profil skapas för att inleda en relation. Förövaren använder ofta en playbook (växlar varmt och kallt – kallar alla samma smeknamn för att lättare hålla många relationer igång). Spelet kan pågå under flera år.

Kombineras ofta med identitetsstöld – deepfake etc – blir mer trovärdigt (vår social-media-användning innebär att vi lägger ut mycket personlig information och bilder som brottslingar kan använda för ett trovärdigt narrativ)

Väldigt vanligt, speciellt efter Covid19. och ett växande problem. Men uppfattas ofta skamligt –stort mörkertal



Denial of Service (överbelastning)

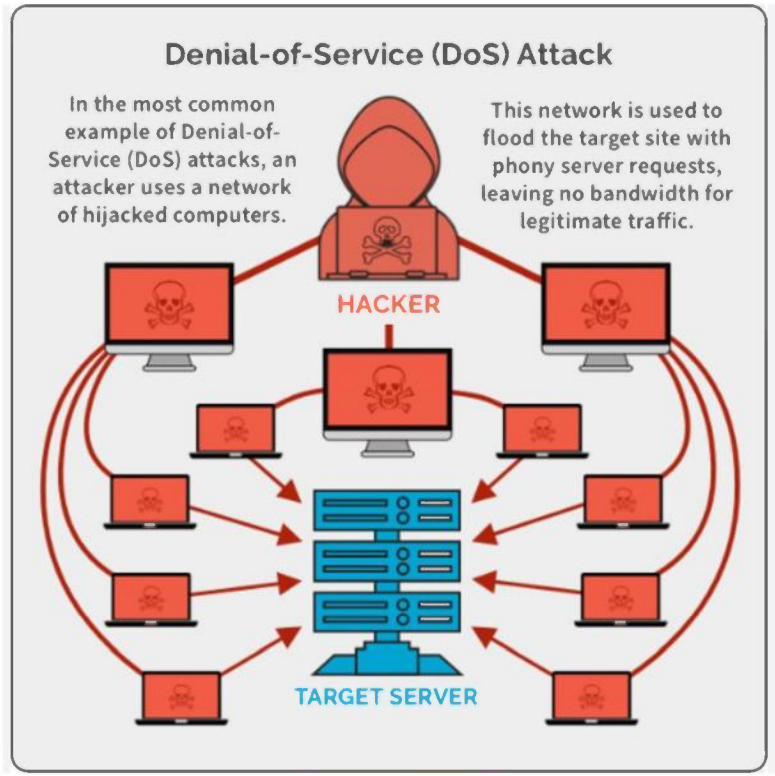
Distributed DoS (DDoS) större skala och högre intensitet

Kommunikation (media, transport) finans-branschen, gaming och e-handel vanliga mål

Exempel 2007 Estland – ledde till 3 v störningar i landets online- infrastruktur

Men många attacker hanteras snabbt: 90% håller på mindre än 10 min

Överbelasning behöver inte vara uppsåtligt. - utan kan uppkomma naturligt när många går in samtidigt på websida ex när SJ släppte sina vinterbiljetter

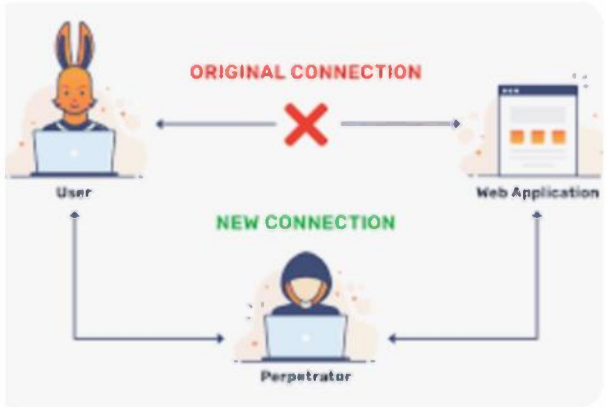


Man-in-the-Middle (MitM) operations

Manipulering av information/ kommunikation mellan ovetande parter, för att ex komma åt information när den skickas /mailas, lyssna in på samtal etc.

Använder sig ofta av en svaghet i systemet för att komma in

Använd kryptering för att skydda kommunikation

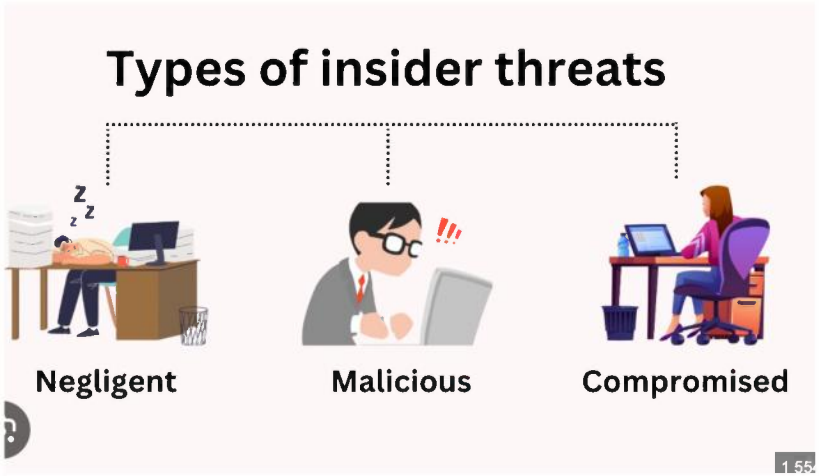


Insiders & hot innifrån

Kan vara en missnöjd anställd, affärspartner som med uppsåt tar information och/eller förstör (malicious)

Men också en anställd som utan uppsåt släpper in någon annan genom att svara på phishing, återanvända läckta passwords etc. (negligent)

eller att en anställds legitima inlog används av någon annnan (informationen har blivit compromised – oftast ovetande)

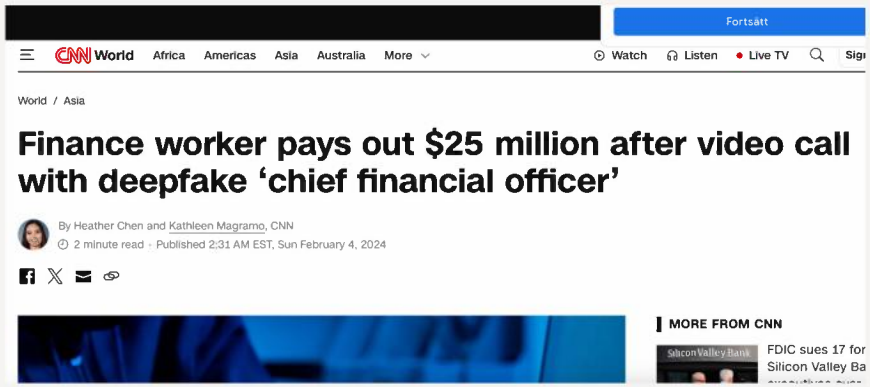


Identitetsstöld & identitetsbedrägeri

I första läget stjäls personlig information – I nästa används denna för att luras. Startar ofta med ett “**breeder document**” ex. Ett ID-kort, som används för att skapa ytterligare dokumentation eller för kreditkort eller start av bankkonton

Vanligt att identitet på barn stjäls för att ligga vilande till barnet är 18

“**Synthetic identity fraud**” kombinerar stulen och förfalskad information –snabbt växande finansiell brottslighet



C-suite fraud (styrgrupp-bedrägeri)

Att kriminella upprättar telefonsamtal och teamsmöten med fejkade arbetskamrater och styrgrupper. Det ser ut, och låter som, du pratar med dina kollegor. Bygger på Deepfake-teknologi som snabbt blivit otroligt övertygande

Nytt fall från Hong Kong- CFO fraud – där en person på ett Teams möte med en falsk ledningsgrupp blir lurad att föra över 25 miljoner dollar

AI-genererade röster ökar också vad gäller telefonsamtal till föräldrar och släkntingar där barn ber om hjälp, eller att betala en lösen på grund av iscensatt kidnappning. Skapar ekonomiska konsekvenser men också stress och emotionell skada

Cryptojacking

Hacka någon annans dator / ta del av annans resurser, för mining av kryptovalutor (använder processkraft - men syftar inte i grunden till att förstöra system eller stjäla information) svårt att upptäcka –märks ofta bara i att systemet blir långsamt

Kryptovalutor särskilt populära i denna värld – pga distribuerat ansvar, och möjlighet till anonymitet (mindre spårbarhet)

'ryptojacking - Blogs UNAH

Advanced Persistent Threats (APTs)

En obehörig tar sig in och gömmer sig i ett närverk en lång tid för att hålla koll, vinna strategiska fördelar

Ofta statliga spelare eller storskaliga brottsliga nätverk

ZERO day

Zero –day (Nolldagars) sårbarhet innebär okända sårbarheter för systemägaren

Zero-day-attacker är alltså sårbarheter som inte har upptäckts eller åtgärdats av den som utvecklat programvaran.

Dessa attacker är särskilt farliga eftersom det inte finns några kända motåtgärder.

Regelbundna säkerhets-genomsökningar och patchhantering är avgörande för att minska riskerna

One-day

En typ av säkerhetshot eller sårbarhet som utnyttjas efter att en sårbarhet har blivit offentlig eller känd av angripare.

Angriparen utnyttjar en redan **känd sårbarhet**, men det har kanske inte ännu släppts (eller installerats) en lösning/fix/uppdatering/ patch

Aktiv exploitering är när angriparen snabbt utvecklar och distrubuerar sårbarheten

Här blir det **tidspress,** eftersom angriparen försöker utnyttja sårbarheten så mycket/ och inom så många organisationer som möjligt - innan de har möjlighet att installera en uppdatering

"one-day" attacker blir farliga eftersom många företag kanske inte har haft tid att åtgärda problem även om de känner till dem

Cybercrime as a Service

Ransomware as a Service (RaaS) är ett vanligt erbjudande

BlackCat (troligt rysk) utförde MGM casino hack 2023 (missad vinst på 100 milj dollar för 10 dagars stillastående)

DarkSide (också troligt rysk) har ett serviceerbjudande med support 24/7, månatlig betalningsmodell, vinstdelning

Evil Corp (rysk) spred Dridex (malware) genom phishing emails till 100-tals banker/finansiella institutioner (40 länder) stal över 100 miljoner dollar

Organisering av kriminella aktiviteter i sofistikerade ecosystem där kriminella kan köpa hacker-tjänster – utan att själva behöva den tekniska kompetensen. De annonserar för nyanställningar på Darkweb där de specar kompetenskrav etc.

Cyberslavar

200 000 personer som tvingas utföra cyberbrott i “scam centers” i SydostAsien (FN rapport, 29 aug 2023)

Cambodia blivit ett center för denna typ av modernt slaveri

Lockade av legitima arbetstillfällen men blir ifråntagna pass placerade i arbetsläger

Vem gör detta och varför

Hotaktörer: Kriminella nätverk; Statliga hotaktörer: underrättelsetjänst (tema 4)

Konkurerande organisationer, olika nätverk, script kiddies, individuella Hackare

Back hats (malicious motives / elakt uppsåt) White hats (intresse av att höja säkerhetsnivå – ex genom att exponera risker // en form av etisk hackning

Varför/ Motiv?

Cyberkriminalitet – oftast ekonomiskt motiverat men kan också vara ideologisk och politiskt.

Komma år hemligheter, tjäna pengar, stoppa verksamhet, sprida lögner (politiskt spel) nationell säkerhet- krigföring

NY
LAGSTIFTNING

VÄRLDEN

Kommer Bryssels regler göra att Europa halkar hopplöst efter?

Uppdaterad 2024-09-23 Publicerad 2024-09-21

8 New California AI Laws *this week*

European Parliament MENU

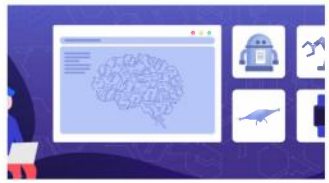
Artificial intelligence

The EU wants to create the right conditions for the development of artificial intelligence and ensure that it works in the interest of Europeans.

Artificial intelligence

EU AI Act: first regulation on artificial intelligence

The use of artificial intelligence in the EU will be regulated by the AI Act, the world's first comprehensive AI law. Find out how it will protect you.



Artificial intelligence

AI rules: what the European Parliament wants

Find out how MEPs are shaping EU artificial intelligence legislation in order to boost innovation while ensuring safety and protecting civil liberties.

Ny lagstiftning

- AI förordningen
- NIS2 direktivet
- CER direktivet
- Cyberresiliens
- GDPR (visserligen inte ny – men relevant)

AI-förordningen

Vem omfattas:

- Tillämplig på alla aktörer som utvecklar, distribuerar eller använder AI-teknik inom EU, oavsett om det är offentliga eller privata organisationer

Innehåll:

- Kategorisering av AI-system i olika risknivåer (hög, medel, låg)
- Strikta regler för högrisk-AI, t.ex. användning av AI inom hälsovård, transport och rättsväsendet, medan lågrisk är tillåtet, på medelnivå är transparens och documentation viktigt

Syfte:

- Att skapa en säker och etisk användning av AI inom EU genom att hantera riskerna kopplade till användning och implementering av AI-system

Krav:

- Krav på transparent användning av AI, ansvarighet och datasäkerhet. Företag måste dokumentera sina AI-system och genomföra riskbedömningar

Böter och sanktioner:

- Höga böter vid överträdelser, upp till 6% av företagets globala omsättning

Oacceptabel risk

AI-system som hamnar i denna kategori utgör ett direkt hot mot individer och är förbjudna.

Hög risk

AI-system som negativt påverkar säkerhet eller grundläggande rättigheter faller in i denna kategori. De är vidare uppdelade i två underkategorier:

- Kategori 1:
  - AI-system som används i produkter som omfattas av EU:s produktlagstiftning för säkerhet (t.ex. leksaker, flyg, bilar, medicintekniska produkter och hissar).
- Kategori 2:
  - Andra högrisk-AI-system som kräver strikt reglering.

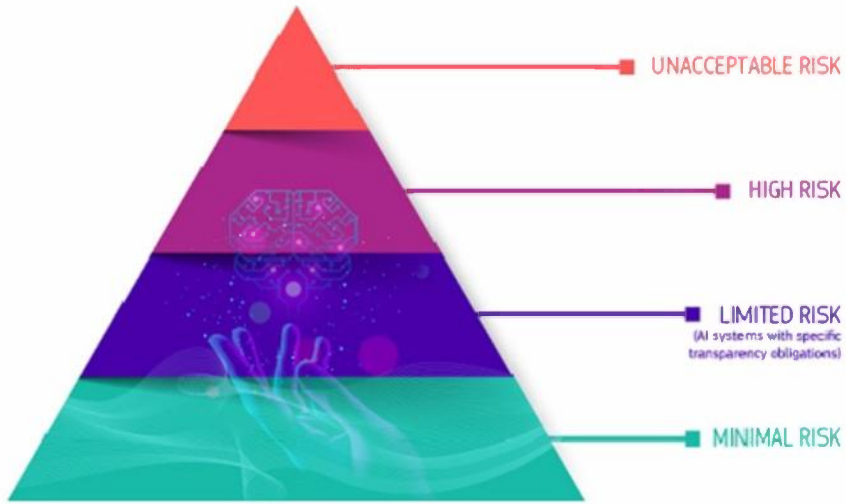
Begränsad risk

AI-system med begränsad risk kan behöva specifika transparensåtaganden för att informera användare om att de interagerar med ett AI-system.

Minimal risk

De flesta AI-system faller in i denna kategori och är föremål för minimala eller inga lagkrav. Dock kan tillämpningen av AI inom kommuners och regioners verksamhet ofta komma att klassas som högrisk-AI.

Olika risknivåer



NIS2 direktivet

Vem omfattas:

- Tillämpas på viktiga sektorer som energi, transport, finans, hälsovård och digital infrastruktur. Företag som tillhandahåller tjänster inom dessa sektorer måste följa reglerna

Innehåll:

- Förbättrad cybersäkerhet för företag inom kritiska sektorer
- Åtgärder för att hantera risker och sårbarheter samt krav på incidentrapportering inom vissa timmar

Syfte:

- Att stärka säkerheten för nätverks- och informationssystem inom EU för att skydda mot cyberattacker och andra säkerhetshot

Krav:

- Företagen ska införa säkerhetsåtgärder, ha en incidenthanteringsplan och rapportera allvarliga incidenter till de utpekade myndigheterna inom varje sektor
- **Böter och sanktioner**:
- Företag som inte följer reglerna kan få stora böter, vilket kan vara upp till 10 miljoner euro eller 2% av den globala omsättningen

NIS2 (forts)

- Verksamhetsutövare ska
  - Identifiera att man omfattas av lagen och anmäla sig
  - Etablera ett systematiskt arbete för informationssälerhet
  - Införa säkerhetsåtgärder
  - Utbilda ledning och personal
  - Rapportera incidenter
- Lagstiftningen är försenad och detaljerna inte helt klara
- Flera remissinstanser har kritiserat att hela verksamheten omfattas – menar att det bara bör vara kritisk del av verksamheten

CER direktivet

Directive on the resilience of critical entities

Vem omfattas:

- Inkluderar både offentliga och privata aktörer som är inblandade i tillhandahållandet av samhällsviktiga tjänster och produkter – ska vara kritiska verksamhetsutövare
    - Verksamhetsutövaren ska tillhandahålla en eller flera samhällsviktiga tjänster inom någon av de utpekade sektorerna (finns i bilagan till direktivet)
    - verksamhetsutövaren ska ha en kritisk infrastruktur belägen i Sverige
    - en incident får en betydande störande effekt för tillhandahållandet av den samhällsviktiga tjänsten.

Innehåll:

- CER-direktivet ska säkerställa att störningar eller avbrott bland samhällsviktiga verksamheter kan förebyggas, motverkas, och hanteras.

Syfte:

- Att skapa ett högre och mer enhetligt säkerhetsnivå över hela EU (IT säkerhet)

Krav:

- Riskbedömningar och genomförande tekniska och organisatoriska åtgärder
- Bakgrundskontroller för vissa befattningar
- Rapportera incidenter

Cyberresiliensförordningen

Vem omfattas:

- Inkluderar både offentliga och privata aktörer som är producerar uppkopplade enheter (produkter med digitala element), hanterar IoT

Syfte:

- Att öka vår motståndskraft för cyberattacker genom uppkopplade enheter

Krav:

- Tillverkare ska säkerställa att deras produkter uppfyller visa krav, under hela sin livslängd och hantera sårbarheter korrekt
- Vid begäran kan tillsynsmyndighet begära in dokumentation att detta är gjort (alltså kunna visa att deras produkter uppfyller de krav som finns)
- Importörer bär ansvar för importerade element
- Rapportera incidenter (24 h) till berörd myndighet

GDPR (General Data Protection Regulation)

Vem omfattas:

- Alla företag och organisationer som hanterar personuppgifter om individer i EU, oavsett var de är baserade

Innehåll:

- Reglerar insamling, lagring och behandling av personuppgifter
- Krav på att informera och inhämta samtycke från individer innan deras data samlas in

Syfte:

- Att skydda individers rätt till privatliv och ge dem kontroll över sina personuppgifter

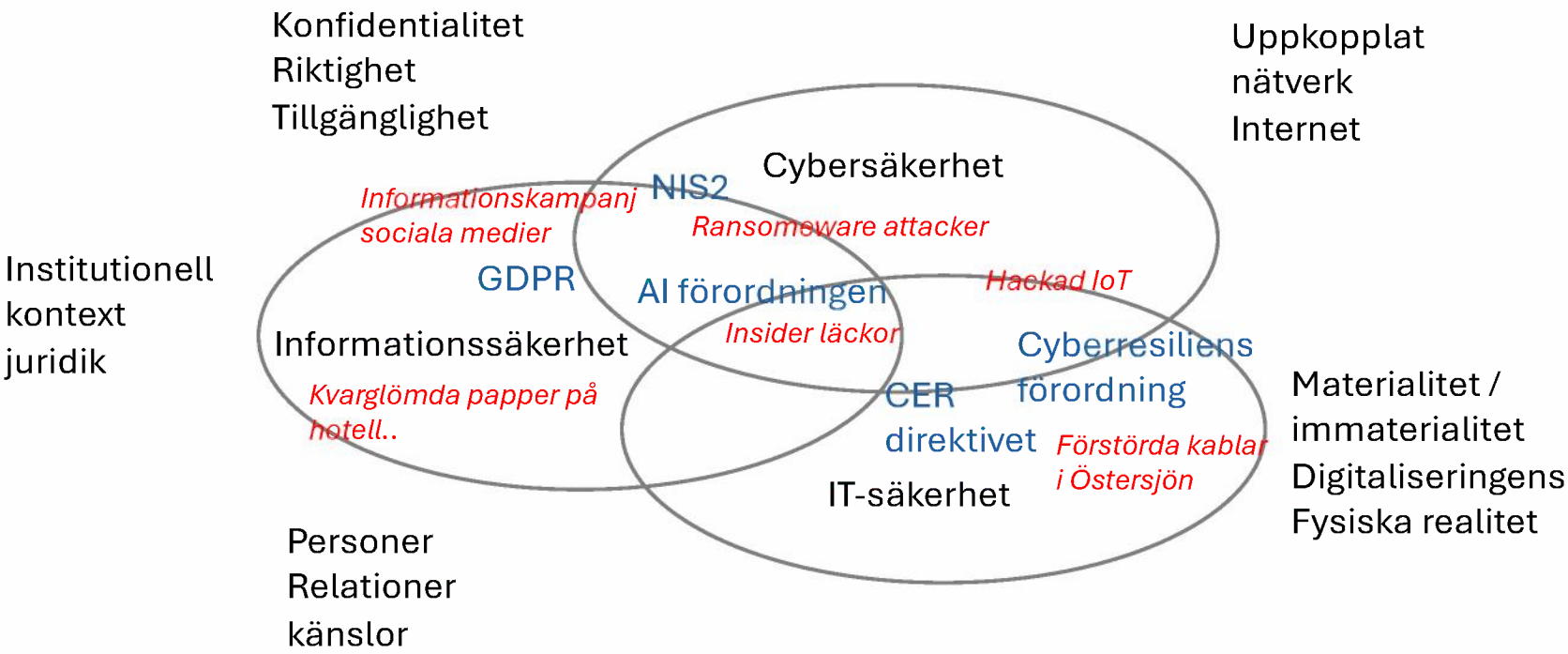
Krav:

- Företag måste införa lämpliga säkerhetsåtgärder för att skydda personuppgifter, och genomföra riskbedömningar vid behandling av känslig data

Böter och sanktioner:

- Böter kan vara upp till 20 miljoner euro eller 4% av den globala årsomsättningen, beroende på vilket som är högst

Concept mapping - del 2



Informationskrig och demokratisk påverkan

- Misinformation (falsk felaktig information)
- Desinformation (falsk och felaktig information med ett syfte – ex propaganda) upprättat för att påverka
- Filterbubblor & Ekokammare - vi exponeras för mer av det vi redan tycker – allt bekräftar vår världsbild
- Algoritmstyrd verklighetsuppfattning
- Polarisering

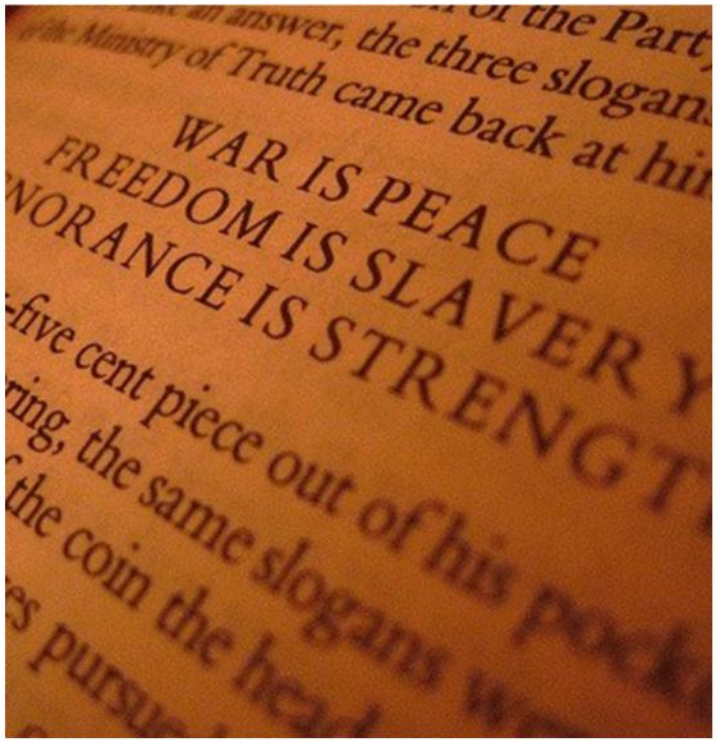
Att samla in och sprida information är centralt både i demokrati och för krigföring.

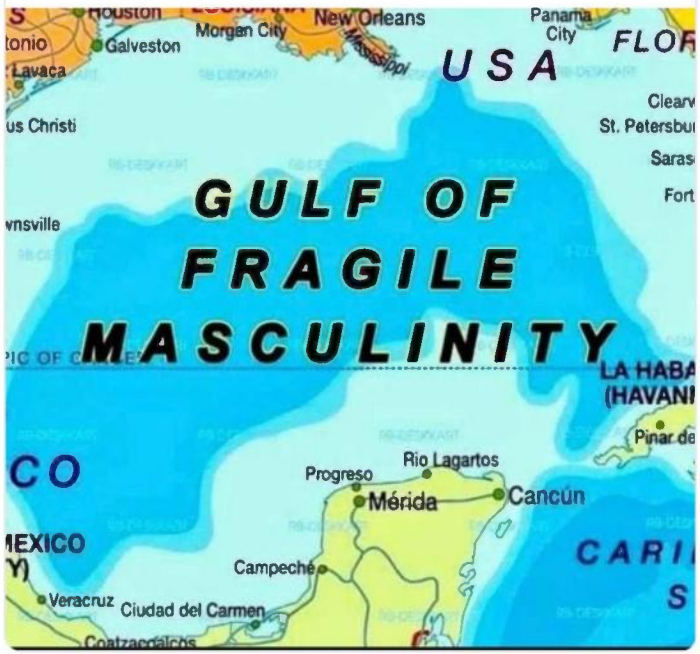
Ett informationskrig pågår för att kontrollera narrativet och uppfattningen om sanning //verklighet

Den som kontrollerar språket kontrollerar tanken

Att kontrollera språket – och tanken

- Orwells 1984 (från 1948) med ständig övervakning och kontroll även över språkbruk och tänkande – new speak
- “Speciell militäroperation” – inte “krig” - Putin
- Gulf of America- inte Mexikanska golfen - Trump
- I USA stryks sådant som gender, homosexualitet, multi-kultur etc ur styrdokument
- I Sverige tas ordet kvinna bort ur abortlagstiftningen – av hänsyn till transpersoner – men försämrar förståelse för lagstiftning speciellt bland svagare utrikesfödda grupper…





Katarzyna Pisarska • Följer
Chair of the Warsaw Security Forum, Chairwoman at the Casimir Pulaski ...
1 d • Redigerad •

I am shocked by all the disinformation that is being spread about Ukraine. Done so in order to convince international publics - especially Americans - that the Ukrainians are loosing the war. THIS IS NOT TRUE.

Here are the facts:

➡️ Ukraine's continues to control 80% of its territory
➡️ Most Ukrainian cities are intact
➡️ Ukraine kills daily 4x as many Russian soldiers as Ukrainian soldiers die.
➡️ Ukraine effectively hits oil and gas infrastructure on Russian territory, curtailing it's production abilities.
➡️ The Russian Black Sea Fleet is gone from Crimea after being decimated by Ukrainian drones.
➡️ Almost 60% of Ukrainians support President Zelensky- and this figure went up since President Trump began to attack him.
➡️ Europe continues to sanction Russia - with the 16th package of sanctions agreed upon last week.
➡️ Sanctions do work - Russian economy is crumbling and urgently needs sanction reflef - especially from Europe!
➡️ We still have almost 200 billion dollars of Russian frozen assets which we can and should give to Ukraine.

Diskussion: Jurister och domstolarnas roll i en tid av demokratisk “backsliding”

Det är viktigt att jurister och domare fortsätter att upprätthålla och försvara rättsstaten //rule of law

Skydda systemen på rätt sätt – söka mer kunskap och börja prata om frågorna
Vi måste ge akt på det som är viktigt och stå emot. Ta Ansvar!

Prata om risker (och möjligheter) i bade professionella och private sammanhang.

Det är viktigt att svara snabbt på eventuella hot/ påverkanskampanjer, men detta är extra svårt för domstolar att göra

Malmö

Malmö stad fejkade it-attack mot anställda – slutade i kaos

6 april 2025 06:00

Tusentals anställda inom Malmö stad utsattes för en fejkad it-attack. Det slutade i kaos. Allt fick avbrytas. Då hade en tredjedel av de anställda redan gått i fällan och klickat på ett fejkat mejl – uppgifter som Malmö stad döljer i sin egen rapport.


Andreas Persson
Text

Lär av brottslingarna...

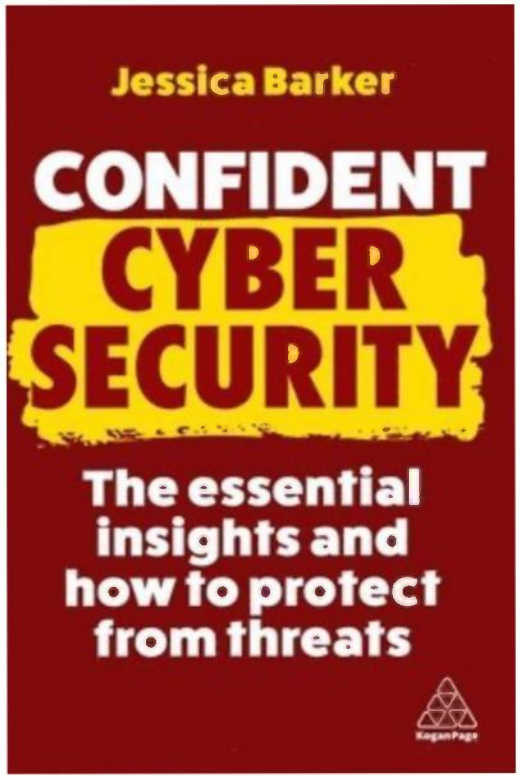
AI Sweden Project: **AI-Powered Honeypots**

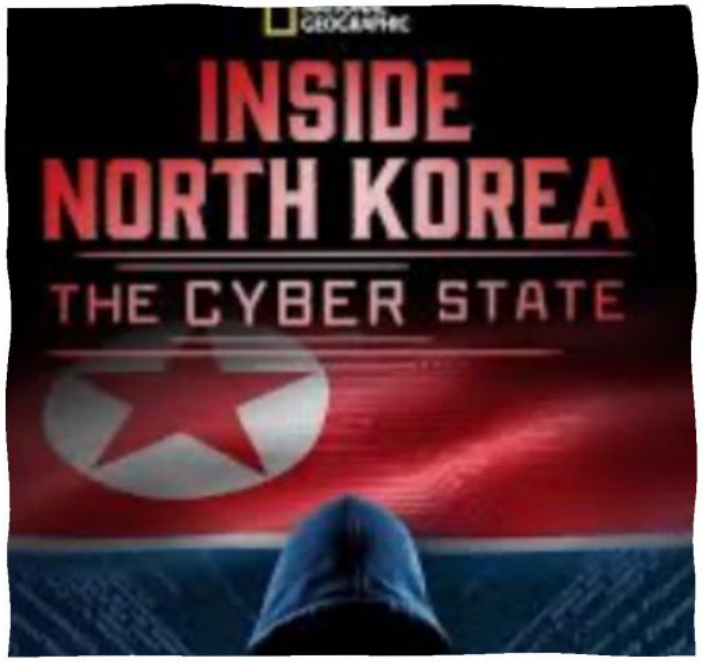
A **honeypot** is a decoy computer system to detect, monitor, and analyze real attacks

Project Goal: Use AI-powered honeypots to trick attackers into showing more of their tools

Partners: Volvo Group, Aixia AB, Scaleout Systems, Västra Götalandsregionen Universitetssjukhuset

Funding: 4M SEK, 06/2024 - 06/2026





Läs- & Filmtips

Kontakta mig gärna på LinkedIn
Eller via mail:
charlotta.kronblad@ait.gu.se