Digitalisering, cybersäkerhet och bevarande av kulturarv – går det att förena?
Keynote speaker: Joakim Brandberg

Hejsan, jag heter Joakim Brandberg och det är väldigt kul att få komma hit.

När jag fick fråga om att prata här om cybersäkerhetsfrågor i en kontext kring kulturarvsfrågor, digitalisering så tänkte jag att det här låter väldigt spännande och det är ju verkligen något som är av betydelse för vårt samhälle i nutid och framtid.

Digitalisering ger nya möjligheter att bevara och tillgängliggöra vårt kulturarv till fler samtidigt som digitalisering innebär nya risker som måste omhändertas.

De senaste åren har de geopolitiska utmaningarna ökat med konflikter i vårt närområde innebär att även vi måste öka vår förmåga och stärka vår beredskap för de fall där även vår nation drabbas.

Hur navigerar vi i det nya landskap som digitalisering och ökade geopolitiska spänningar innebär?

Om vi ser till samhällsutmaningen med digitaliseringen så är det verkligen en multidisciplinär utmaning där perspektiv från olika yrkeskompetenser är avgörande.

Jag tänkte mig att försöka, utifrån mitt perspektiv, att sätta in cybersäkerhet i detta sammanhang.

Inte helt enkelt men jag ska försöka iallafall.

Så det kan vara intressant för er att känna till lite om vad jag har med mig i mitt bagage erfarenhetsmässigt.

Jag har arbetat med informationsteknik i hela mitt liv efter att jag blev klar på universitetet, min inriktning är "digital", det vill säga alla tillämpningar som jag arbetat med har till väldigt stor del utgått från att fysiska manifestationer realiseras med hjälp av informationsteknik och/eller interagerar med en fysisk verklighet s.k cyberphysical (cyberfysiska) system, t ex vattenverk och moderna bilar som ju skulle kunna beskrivas som en ipad på hjul i en del fall.

Jag är egenföretagare, gift pappa 50+ med tonårsbarn och samhällsmedborgare.

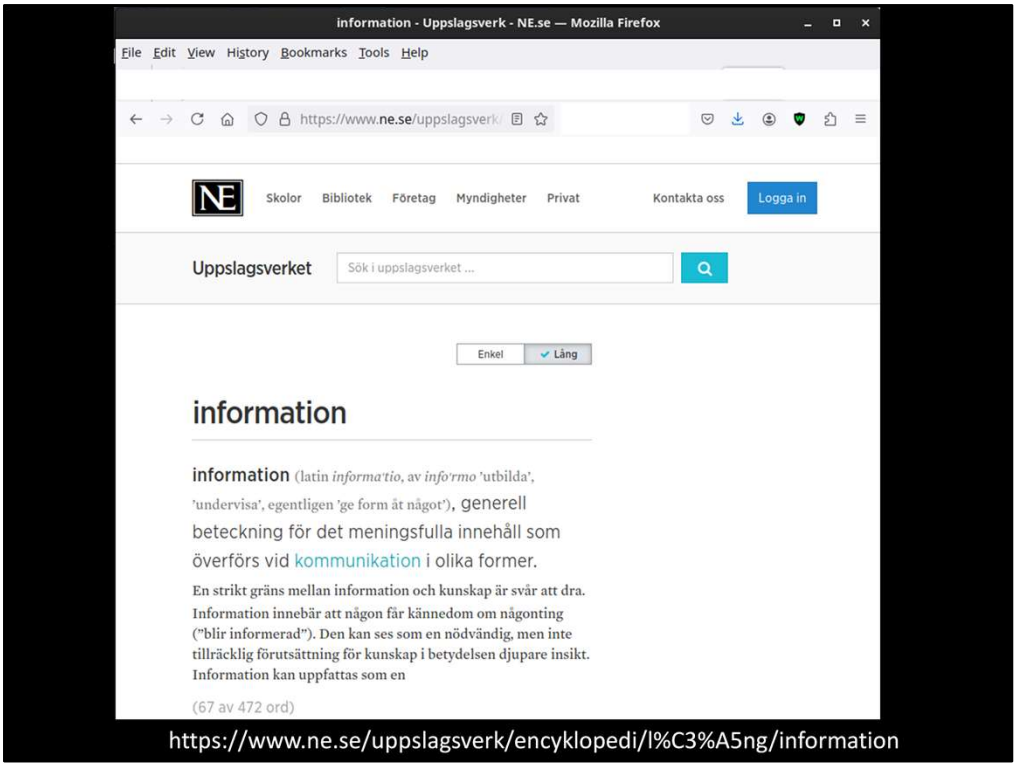
Jag har mina tidigare erfarenheter som CISO, reservofficer, forskare, ingenjör med mera. Mina erfarenhet kommer från verksamheter där frågor som arkivering och bevarande på lång sikt med samhällshorisont kanske inte har legat högst på prioritetsordningen, däremot har jag praktiskt stött på och aktivt arbetat med och försökt påverka dessa frågor när jag har haft förmånen att kunna göra det.

Jag har sedan mer än 25 år tillbaks jobbat inom samhällsviktiga och säkerhetskänsliga tillämpningar med fokus på informationssäkerhet eller som jag hellre säger möjliggörande av verksamhet i en digital kontext där hotbilden är hög och konsekvenserna blir stora om det går åt pipsvängen.

Så digitalisering det är tidens melodi.

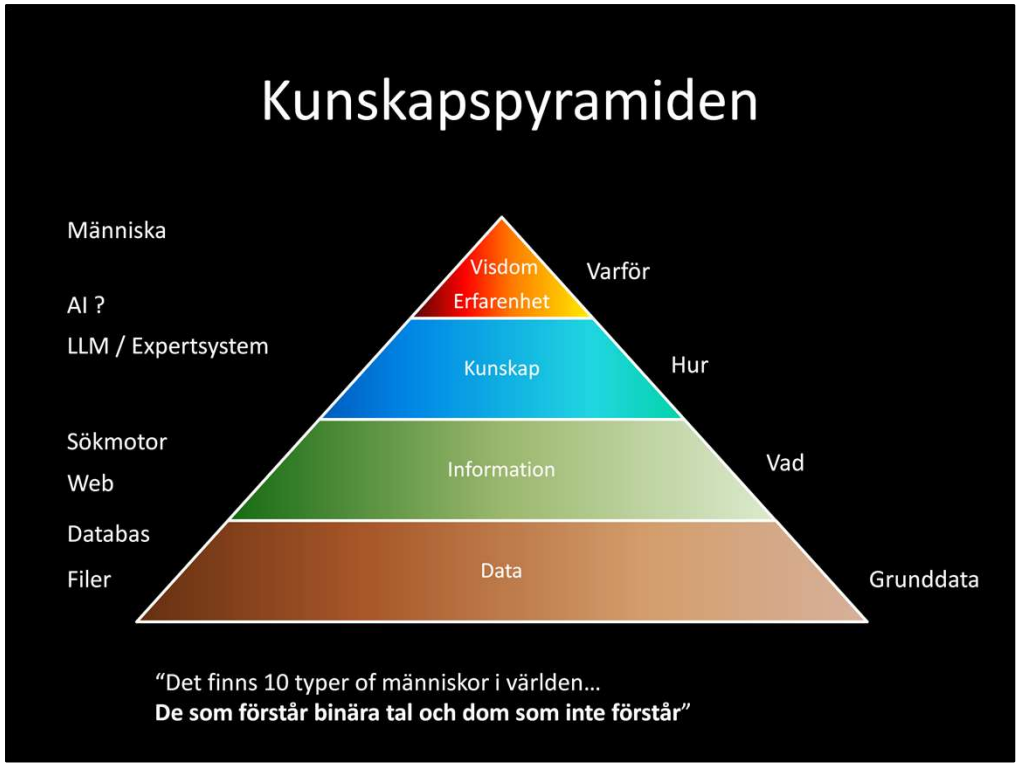
Jag ska inte försöka mig på att göra en definition av begreppet som innehåller så mycket olika nyanser.

Däremot så kan jag konstatera att digitaliseringen av samhället producerar information, och just begreppet information vill jag börja med att ägna lite tid åt.



Vad menas egentligen med information?

NE definierar information som en generell beteckning för det meningsfulla innehåll som förs över vid kommunikation i olika former.



Inom IT beskriver man ofta information med hjälp av kunskapspyramiden och modellerar med 4 nivåer, data , information, kunskap, visdom/erfarenhet.

Jag har placerat några digitala artefakter till vänster i pyramiden men rent krasst utifrån detta sättet att dela in "information" så finns det idag inga IT-system som klarar den högsta nivån visdom/erfarenhet.

Det här är ett försök att genom en modell för visa hur de högre lagren i pyramiden beror på varandra och att det blir "mindre" mängd information ju högre upp man kommer, samt att kontexten minskar ju längre ned man är i pyramiden.

Det är ett inte helt oproblematiskt sätt att se på verkligheten om man tänker efter, då data, helt för sig själv renodlat kan vara mycket svårt att få något egentligt sammanhang ur.

Kunskap ses ofta som något som är användbart och tillämpligt i en given kontext.

Men med detta perspektiv så är själva kunskapen knuten till "dom som kan" och om man inte har några som kan så minskar ju den praktiska nyttan av kunskapen.

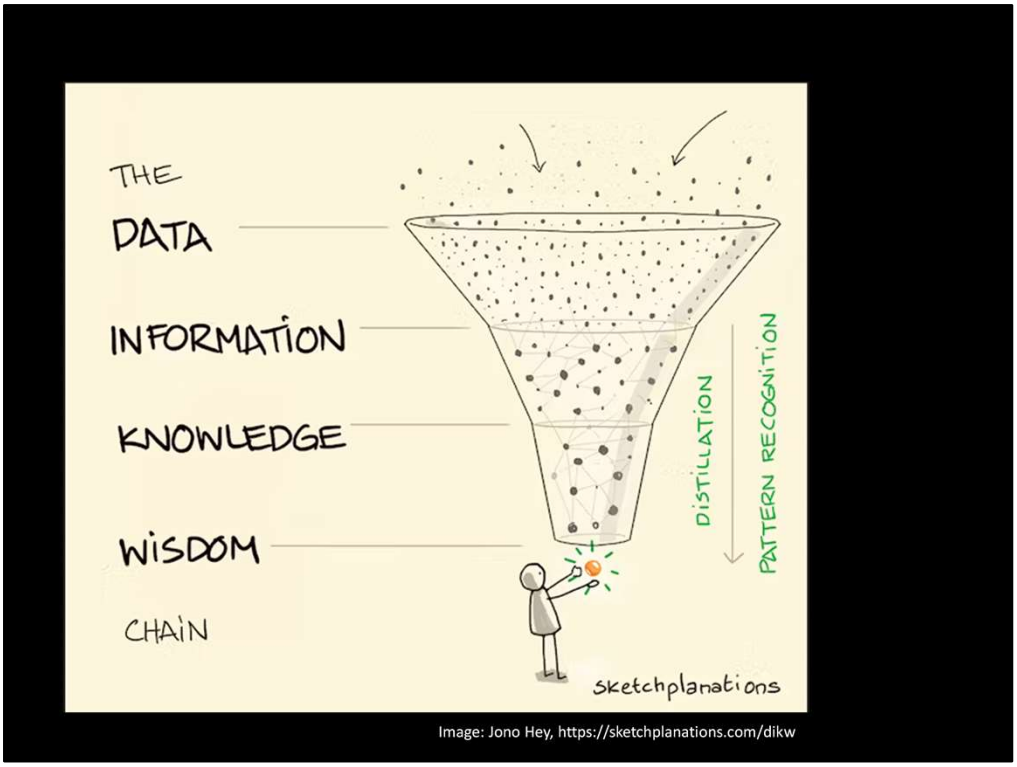


Image: Jono Hey, https://sketchplanations.com/dikw

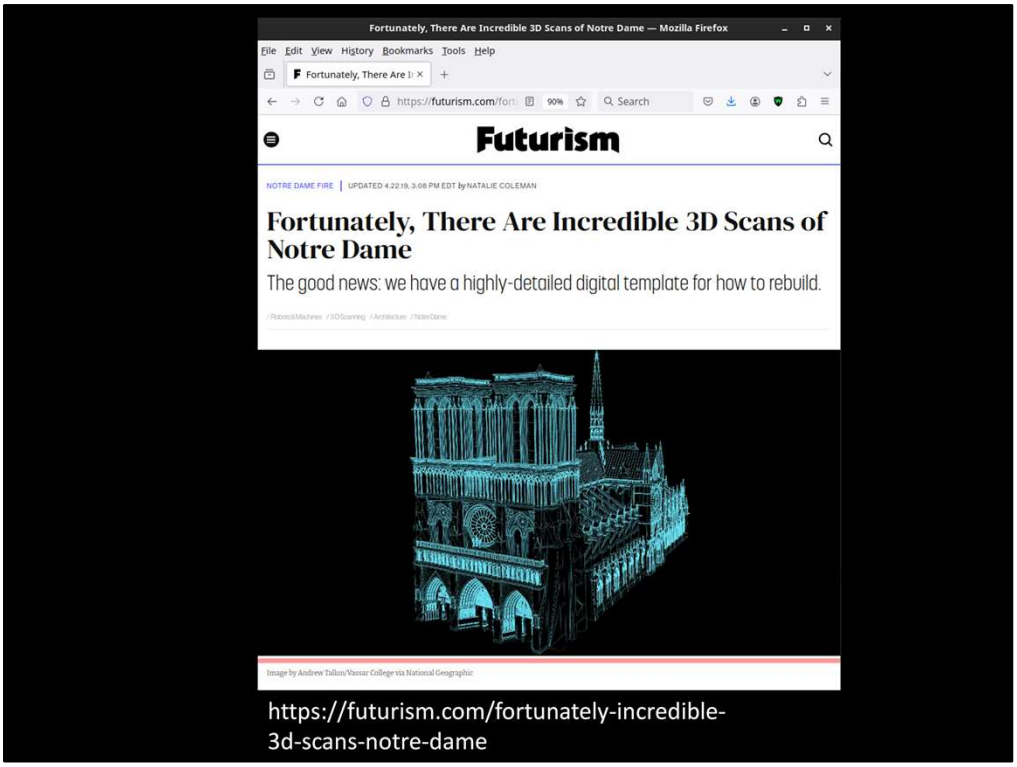
Så åter till digitalisering. Jag tänkte mig separera två distinkta användningsfall.

Det ena är att använda tekniken för befintliga artefakter och hälla i dem i digitaliseringstratten för att skapa något digitalt.

Syfte kan skilja men det kan tex vara att minska kostnaderna och kanske till och med kunna minska exponeringen och degraderingen av den aktuella fysiska artefakten genom att den får ligga orörd och därmed få den bevarad längre och bättre.

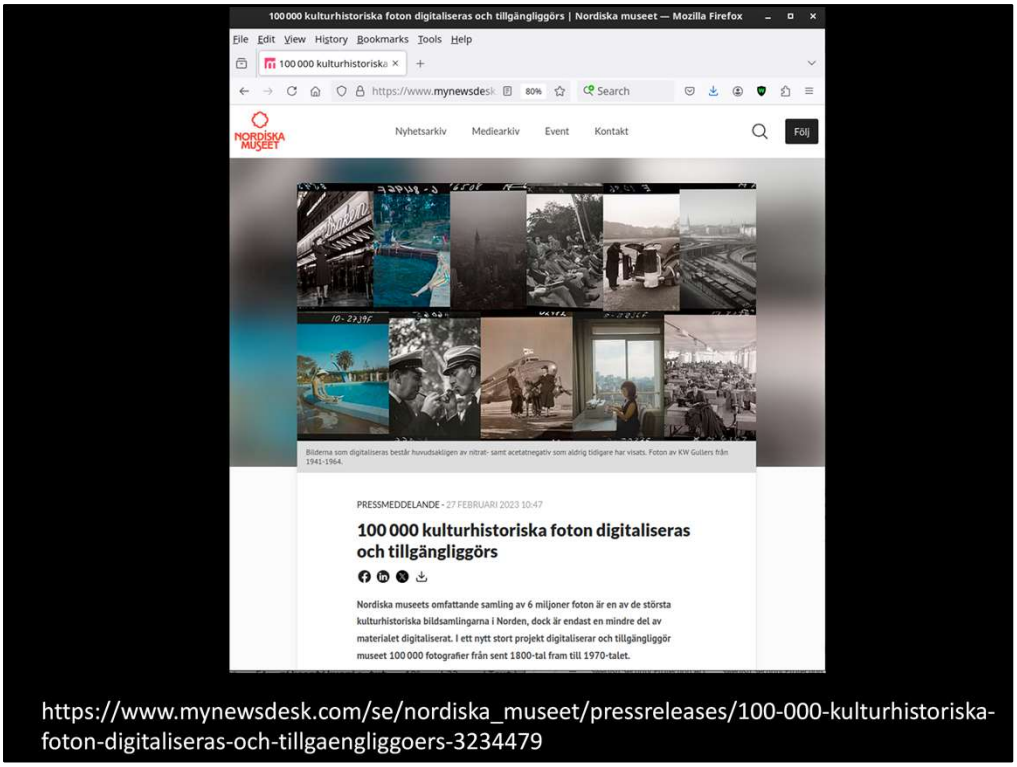
Ett bra exempel är att från gamla dokumentkällor att skapa digitala arkiv.

När informationen väl är digital så kan man ju sedan använda sig av Machine Learning och tolkningsalgoritmer för att upparbeta informationen ytterligare t ex i släktforskningsfallet, skapa genealogier per automatik på allt som har digitaliserats.



Att använda sig av teknikens möjligheter kan också skapa en sorts backup/hjälp/stöd om det nu skulle vara så att det som inte får hända händer.

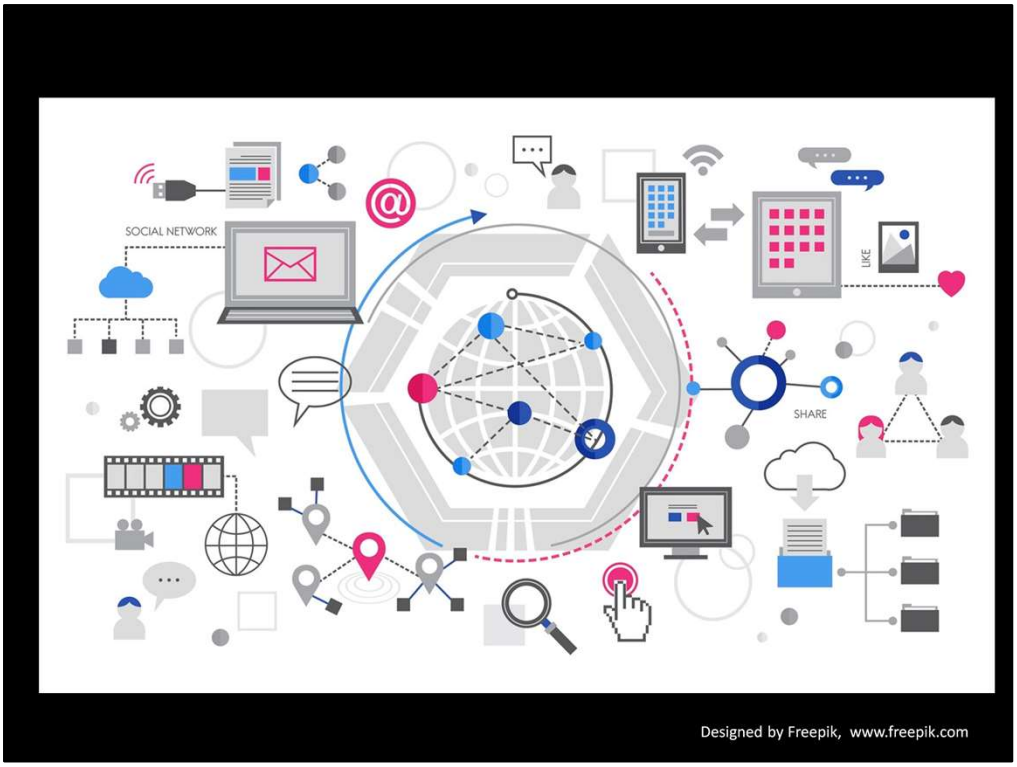
I efterspelet av branden i Notre Dame 2019 så visade det sig att en 3D-scanning av byggnaden som gjorts, har hjälpt avsevärt under restaurationsarbetet.



https://www.mynewsdesk.com/se/nordiska_museet/pressreleases/100-000-kulturhistoriska-foton-digitaliseras-och-tillgaengliggoers-3234479

Nordiska museet drabbades av vattenskador vilket nu lett till att många fler får möjlighet att ta del 100000 foton som annars hade varit svårt att kunna ta del av.

Så å ena sidan har vi möjligheter i och med digitalisering att ta fysiska objekt som sedan kan visas i en digital omgivning och å andra sidan



alla nya sätt som uppstår med hjälp eller på grund av informationsteknikens framfart och det är här som känslan av fartvind i håret uppstår.

Ur ett perspektiv så går det fort med alla system, chat, LLM, sociala media, influencers, insta, tiktokare, gamers osv, osv, och subkulturer som uppstår i kölvattnet av dessa företeelser.

Men ur ett annat är det som det alltid varit, vi är människor som är sociala varelser och som söker kontakt, bekräftelse och intryck genom interaktion med varandra.

Vi lever idag i en digital stenålder enligt min uppfattning, det kommer inte vara mycket kvar för någon att studera om 100 år, det räcker till och med att säga 10 år om man är lite mer pessimistisk och det finns ju goda förklaringar till varför det är som det är.

På många sätt beror ju framgången med internet och dess företeelser på just det faktum att regleringen har varit låg och att det bygger på att den som vill bidrar med det den kan.

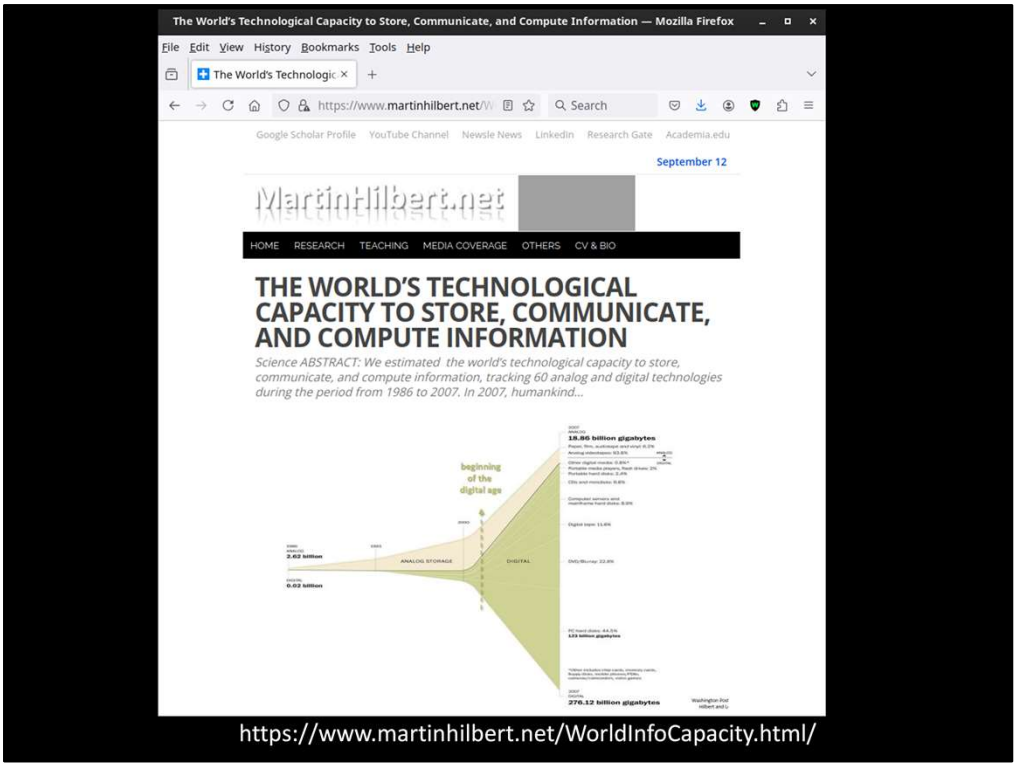
Fråga: Ska vi verkligen bevara digital information?

Svar: Om nu all denna information nu är värd att producera från första början så är säkert något av den värd att bevara.

Frågan är bara vad ska vi bevara…

För att börja kunna ta ställning till detta så tänker iallafall jag

Hur mycket information genererar vi och lagrar i världen då?



Och det är inte så lätt att svara på men 2011 så publicerades en studie i Science.

Studien ger en bild av hur informationstillväxten ökat mellan 1986 och 2007 pga digitaliseringsförmågan. Den visar 2 trender, det skapades mer och mer information och av mängden information som genererades, kommunicerades och lagrades 2007, var mer än 90% digital, idag spekulativt är vi nog i ett läge där mindre än 1% av informationen är "analog".

Ytterligare en frågeställning uppstår nu:

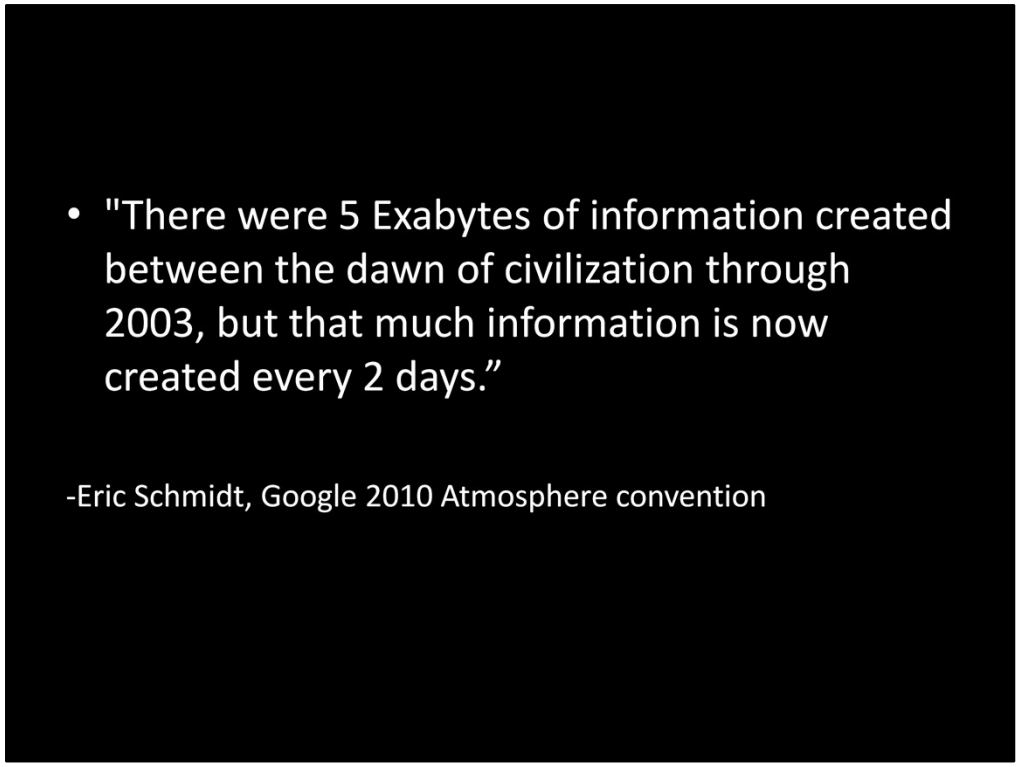
Om vi tänker oss all information som producerats och lagrats i någon form sen civilisationens ursprung innan digitaliseringens start

Hur mycket är det?

Och när passerade vi gränsen för när vi börjar producera mer än så varje år?

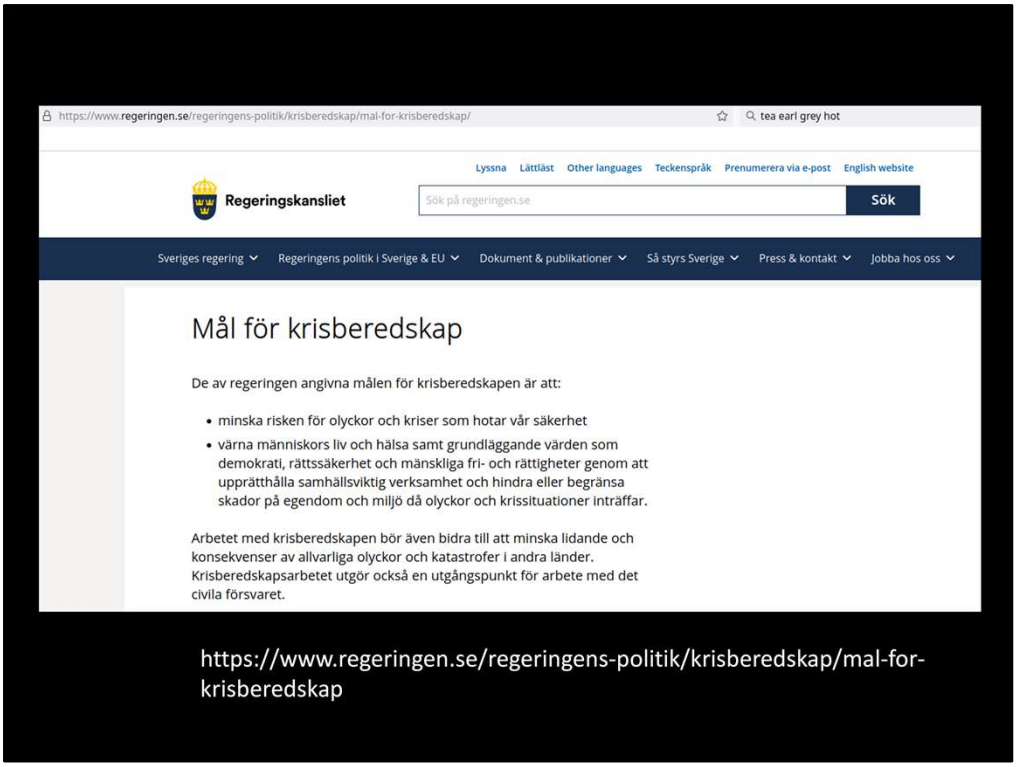
Trenden ger ju vid handen att det förmodligen redan inträffat.

Det var inte enkelt att hitta.



Men Googles VD, Erich Schmidt hävdade att vi 2010 generade lika mycket information varannan dag som vi genererat från civilisationens begynnelse till 2003.

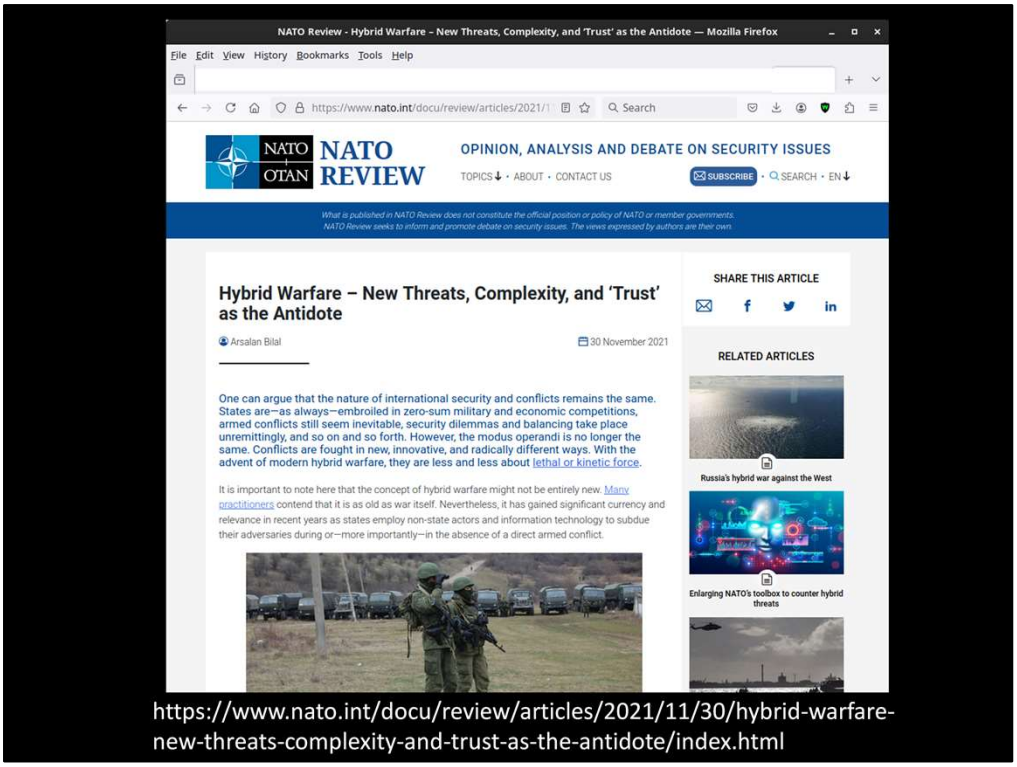
Jag måste varna och påpeka att exaktheten i detta citat ska och kan ifrågasättas men visar det iallafall på magnituder i förmågan att generera information i dagens tider.



Från att ha varit relativt avspänt i vår del av världen under ett antal decennier efter att muren föll så har läget ju blivit ett helt annat och satt förstoringsglaset på inte minst vårat samhälles försvarsförmåga.

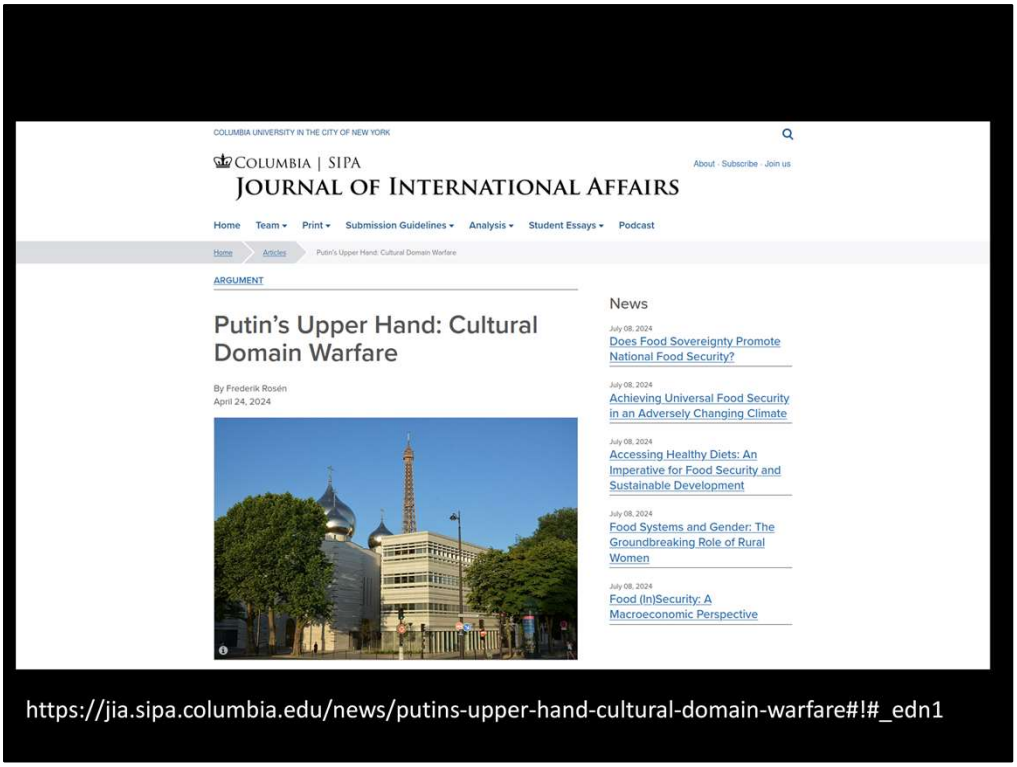
Att arbetet med vårat kulturarv är en samhällsviktig verksamhet och ska försvaras är inte någon skräll med tanke på RK:s formulering.

Däremot så är det enligt min uppfattning inte det mest prioriterade av alla samhällsviktiga och för den delen säkerhetskänsliga verksamheter som bedrivs i Sverige.



https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Rysslands annektering av Krim 2014 har satt hybridkrigföring på samhällsagendan



https://jia.sipa.columbia.edu/news/putins-upper-hand-cultural-domain-warfare#!#_edn1

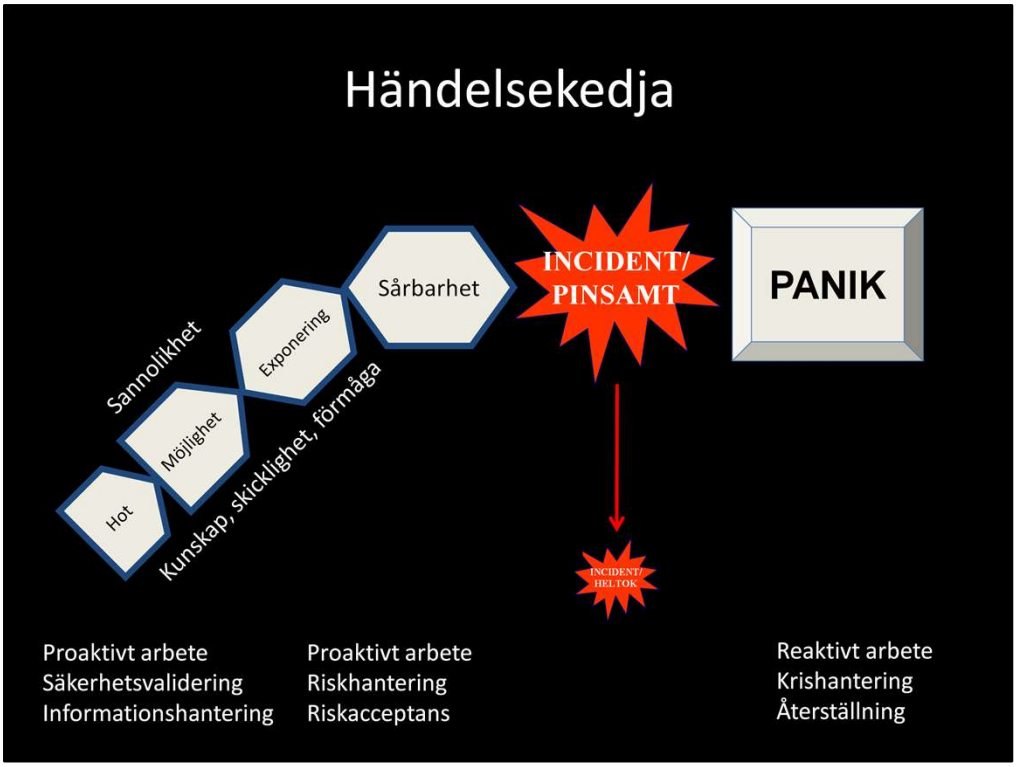
Hybridkriget sker inom olika samhällsarenor och verkar i många fall i en ”gråzon” inom ramen för (framförallt) staters intressen i vad som vi betecknar fredstid.

Syftet är att påverka förtroendet eller om man så vill tilliten till samhällets förmåga och därmed minska samhällets motståndskraft.

Detta hot måste tas på allvar!

https://www.economist.com/culture/2022/03/19/vladimir-putins-war-endangers-ukraines-cultural-heritage

Ett väldigt aktuellt exempel är kriget i Ukraina där det är väldigt tydligt att påverkan på kulturarv är ett av målen i krigföringen.



Nu har jag försökt måla med den breda penseln och om man nu för in cyberperspektivet i den här kontexten, vad ska man nu fokusera på?

Enligt min uppfattning så handlar det om att fortsätta med att hantera samma saker som förut med tillägget att cyber tillför ytterligare komplexitet.

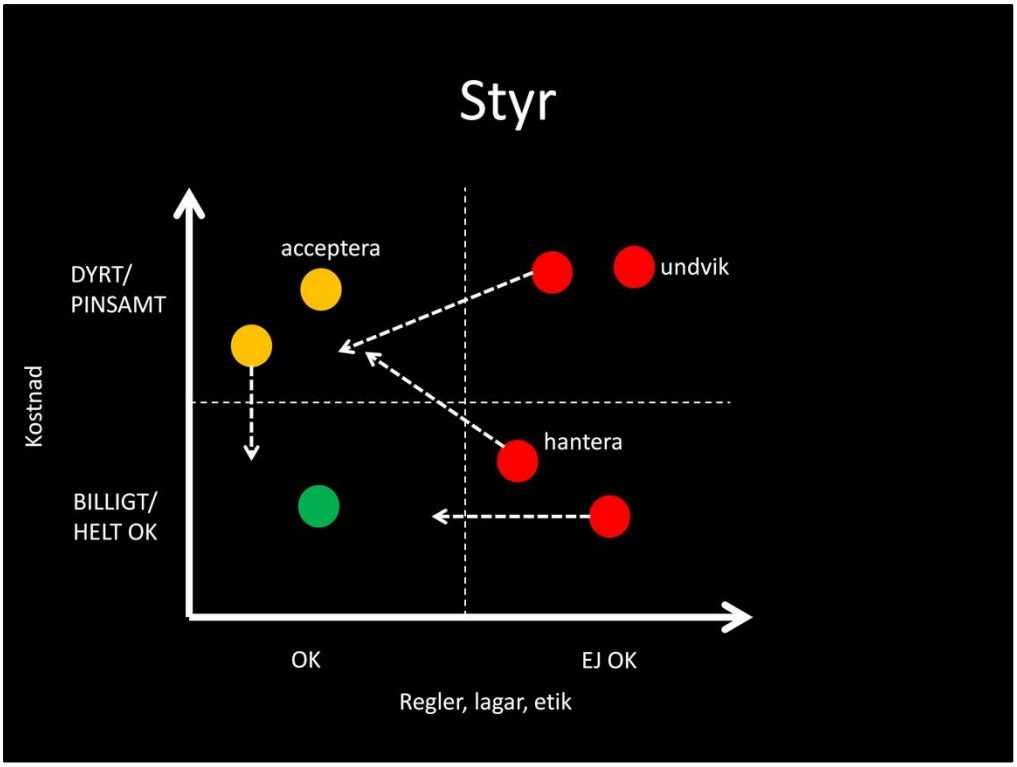
Mer och mer värdebärande artefakter kommer att vara digitala, hotaktörer har fördelen av att i många fall slippa behöva åka till objektet av intresse.

De kan istället sitta i lugn och ro på andra sidan jorden med väldigt låg upptäcktsrisk och genomföra sin verksamhet.

Det är svårare att se vad som hänt när eller om man väl upptäcker att det hänt något.

Det vi vill undvika och helst minska är konsekvenser som uppstår när det som inte får hända händer.

Det finns mycket man skulle kunna prata om kring hur man skapar en bättre cybersäkerhetsförmåga men jag vill peka på tre saker som är centrala.



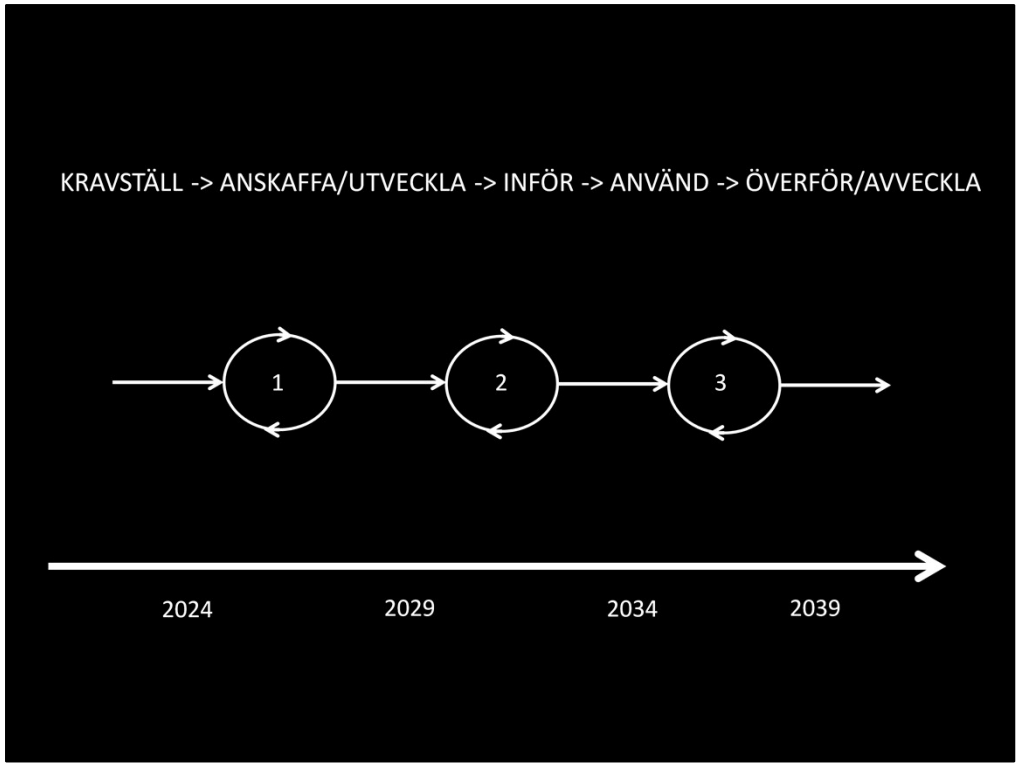
Nummer ett:
Styr verksamheten, prioritera risker tala om vad som är ok och vad som inte är ok.

Precis som allt annat så går det inte att skydda sig mot allt eller för den delen uppnå en hundraprocentig säkerhet.

Då blir det viktigt att välja och därefter kommunicera vad vi prioriterar och för den delen inte prioriterar. En sån här övning utgår naturligt utifrån de tillgångar som finns och att utifrån de risker/händelser man identifierat visa en tydlig inriktning.

Att göra en riskacceptansmatris är en alldeles utmärkt övning. Den går ut på att placera riskerna i en klassisk fyrfältare och därefter ange vad som är ambitionen med risken.

Min erfarenhet att just denna typ av övning är relativt ovanlig men den kan verkligen bidra bidrar till att ta bort otydligheter när man väl arbetar med ett specifikt område.

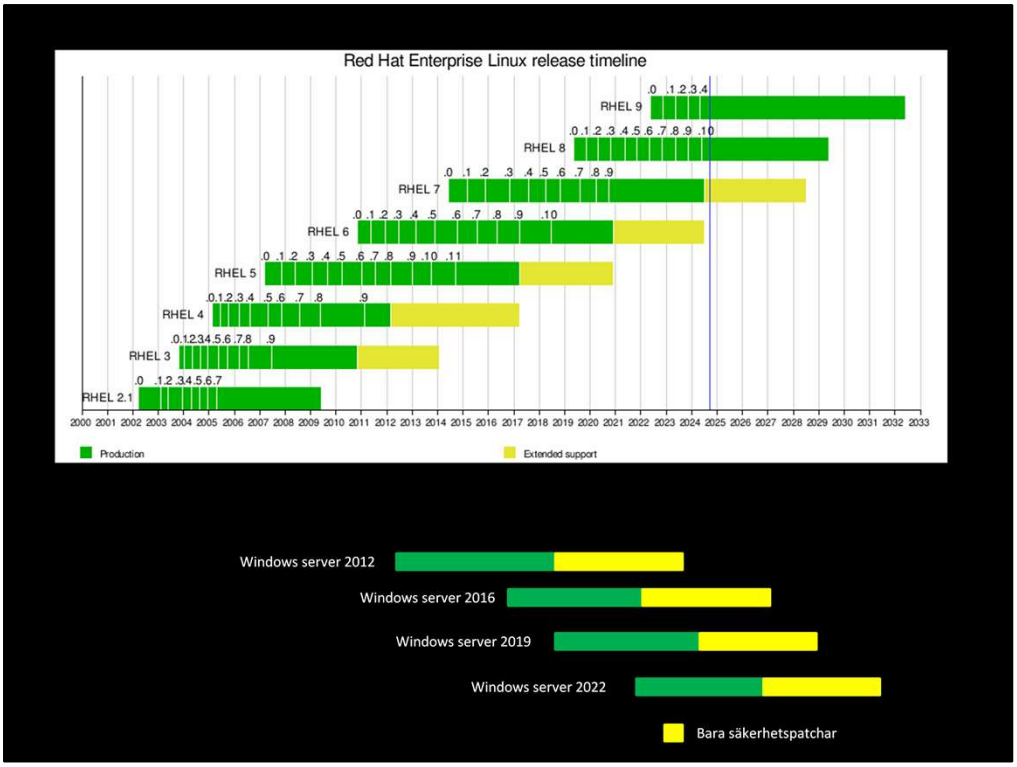


Nummer 2:
Tänk på att det digitala hantverket.

I något sorts historiskt användningsperspektiv så är tekniken på stenåldersnivån.

Man får inte glömma att inom digitaliseringsområdet är vi i en expansionsfas av teknik och till och med teknologi där fokus är på att hitta på nya saker att tjäna pengar på.

Det innebär att den tekniska livslängden är mycket kort i ett samhällsperspektiv. I server-driftcentralsfallet ligger cykeln på cirka 5 år för hård- och grundläggande mjukvara (operativsystem med mera). Ur ett praktiskt perspektiv ger detta cirka 3-4 år produktionstid per generation om man tar hänsyn till införande och migrering. Är verksamheten kontinuerlig över tid är detta något som måste hanteras i och med att den teknik som fallit ur tiden och inte ligger i fönstret för utveckling/support inte längre rättas och därmed blir hopplöst osäker med tiden.

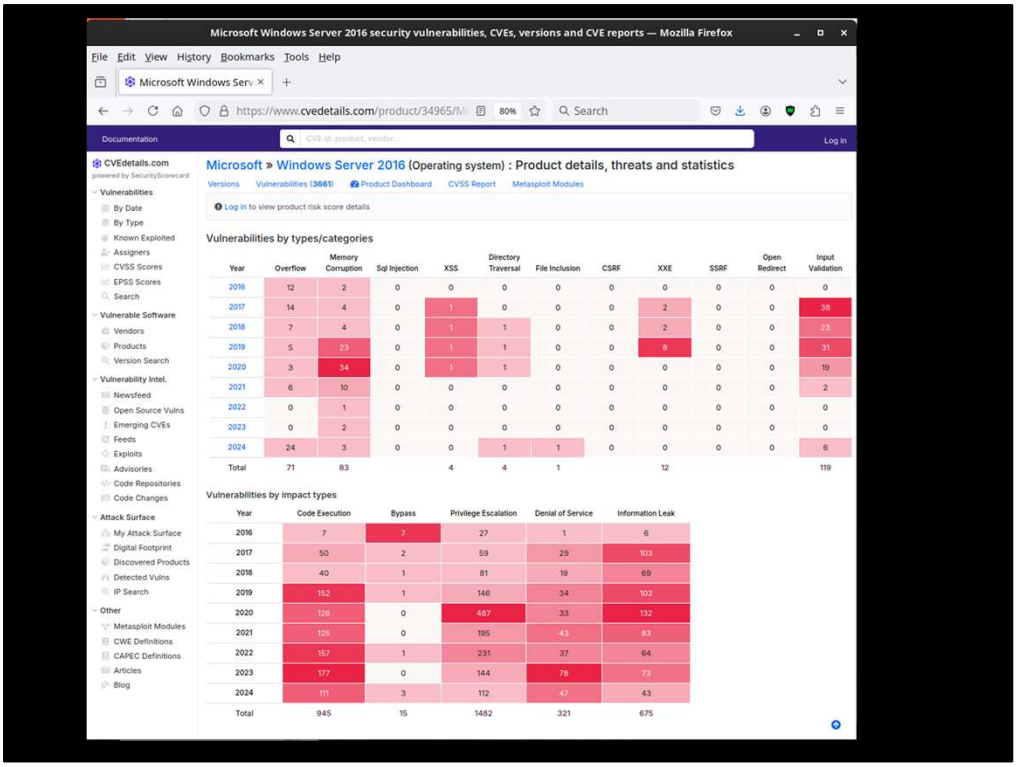


Här är livscykeln för två kommersiella operativsystem, Red Hat Enterprise Linux, numera IBM och Microsoft Windows.

I de gröna fälten är systemen aktivt underhållna, i de gula kommer endast säkerhetsrättningar.

Så här står man lite som åsnan mellan två hötappar. Ska man köra det senaste (och säkraste) operativsystemet och åka på alla barnsjukdomar eller ska man vänta.

Att komma in i det gula fältet är starten på ett sluttande plan nedåt då systemet bara blir sämre , osäkrare och dyrare.



Om man tittar på säkerhetsrapporter för Windows 2016 så ser man också tydigt att mängden upptäckta brister tilltar med viss eftersläpning och detta beror på bl.a att det är färre som kör ett nytt OS precis när det är släppt. Inte nödvändigtvis betyder detta att det är säkrare I början. Bara att det är färre ögon som kan upptäcka fel.

Windows 2016 är ju på väg ut nu och supporten upphör Januari 2027 så just nu kommer det bara säkerhetsuppdateringar om man inte väljer att specifikt betala extra för andra typer av rättningar.

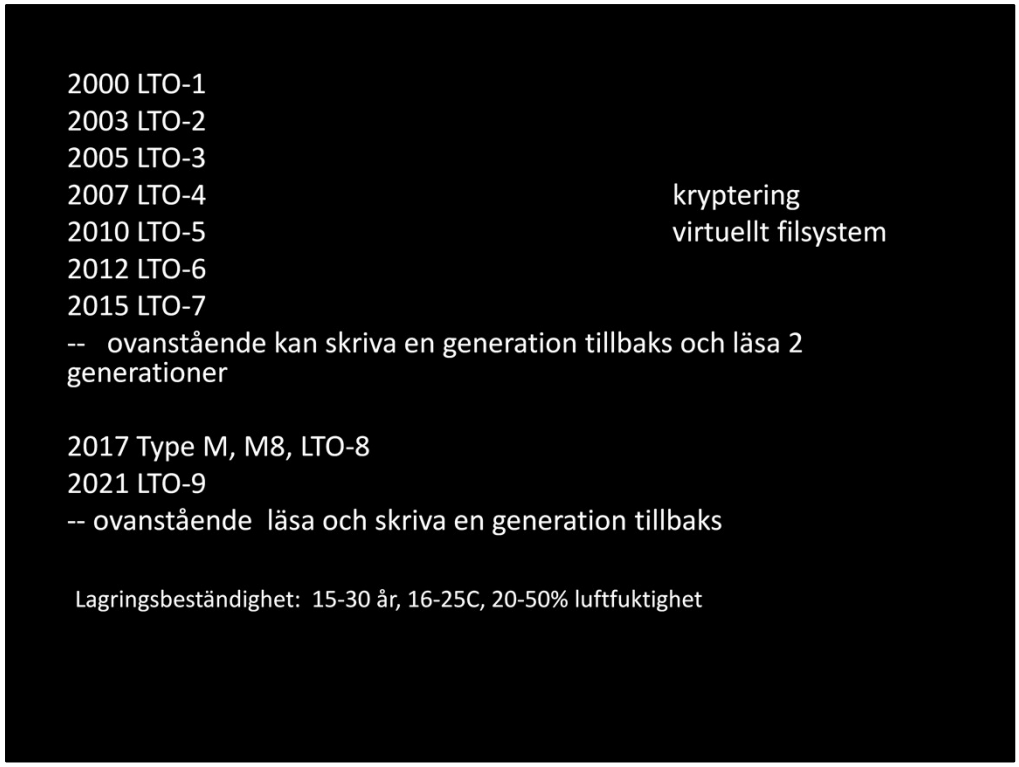
1725, Hålkort/remsa, Bouchons vävstol, Musée des Arts et Métiers, Paris
1951, Band (Magnetic tape), UNIVAC I, EMCC
1957, Hårddisk, (1954) , IBM 350 (RAMAC)
1971, Floppydisk, 8” IBM 23FD
1985, Magneto optical disk, Kees Schouhamer Immink and Joseph Braat
1985, CDROM, ISO/IEC 10149
1991, Solid state disk, SSD, StorageTek
1994, Compact flash, Sandisk
1995, Zip drive, Iomega
1996, DVD, Sony, Panasonic, Philips, Toshiba
2000, Linear tape open, LTO, IBM, HP and Seagate formed the LTO Consortium
2000, USB Flash drive, flera uppfinnare (tvist)
2006, Blueray, Sony, Blu-ray Disc Association
? ,Cloud storage

Källa, wikipedia

Här ser vi några av de sätt som vi använt oss av när det kommer till att spara digital information på ett media som inte är flyktigt.

Redan 1725 så uppfanns hålkortet/remsan och det var ett av de första sätten som vi använde oss av när den moderna datorn började användas. Därefter har vi passerat ett antal teknologier baserade på olika metoder.

Optiska, magnetiska och transistorbaserade medier är dominerande sedan 20 år tillbaks.



Om vi tittar närmare på Linear Tape Open, LTO som är en dominerande teknik för att idag lagra information på band t ex när man tar backup på information för att kunna ha den off-site i händelse av att den primära driftcentralen slås ut.

Det har kommit 9 generationer av LTO sedan år 2000 och det är planerat ytterligare 5 enligt vad man kan se idag på LTO consortiums hemsida.

Så en ganska svår frågeställning här angående arkivbeständighet uppstår iallafall för mig.

Det är iallafall inte bara att spara banden i 30 år och tro att man kan få tillbaks informationen.

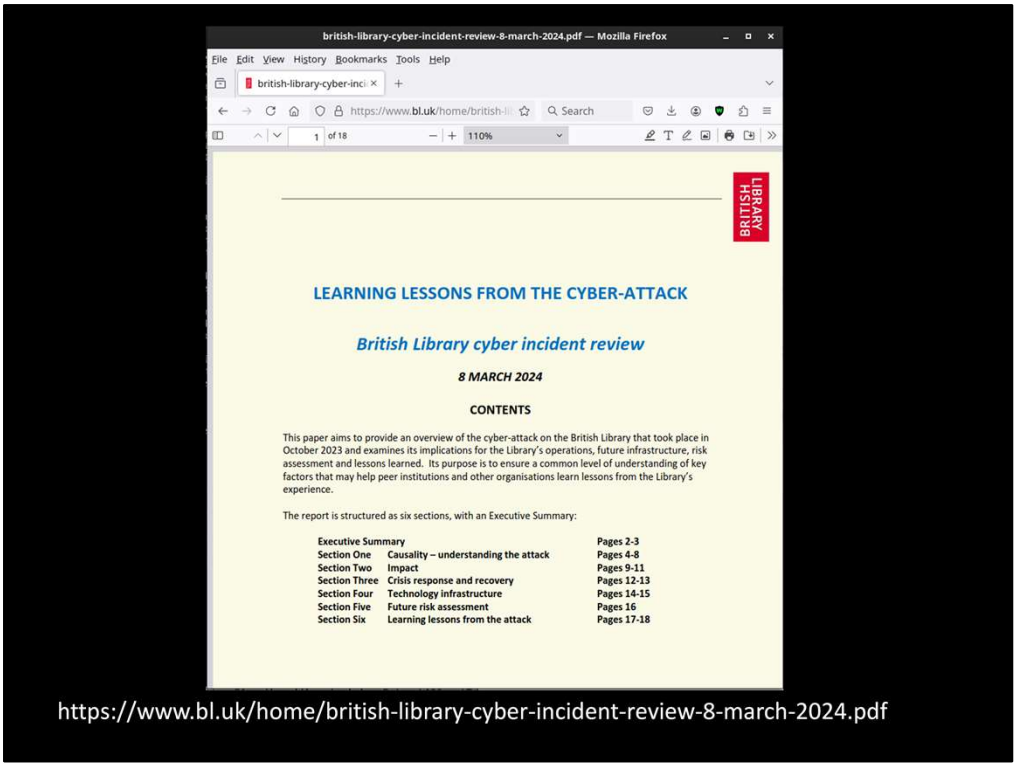
Nummer 3:
Använd er av erfarenhet inom andra områden, exempelvis kritisk infrastruktur och nationell säkerhet.

Krasst kan man säga att det mesta som behöver skrivas inom informationssäkerhet och it-säkerhet på ett tag, redan är skrivet.

Den stora utmaningen är att börja göra som det faktiskt står skrivet.

Jag ska inte gå in på detta djupare då det är som en kollega sa till mig en gång:
"- Fasen, det du håller på med är ju så torrt att det självantänder".

Men en bra startpunkt är Myndigheten för samhällsskydd och beredskap samt säkerhetspolisen som ger ut föreskrifter för samhällsviktig- och säkerhetskänslig verksamhet. De har även gjort vägledningar för hur man ska tolka dessa.



Jag tänkte istället att gå igenom en fallstudie nämligen en cyberattack som British library drabbades av för ett år sedan i oktober 2023.

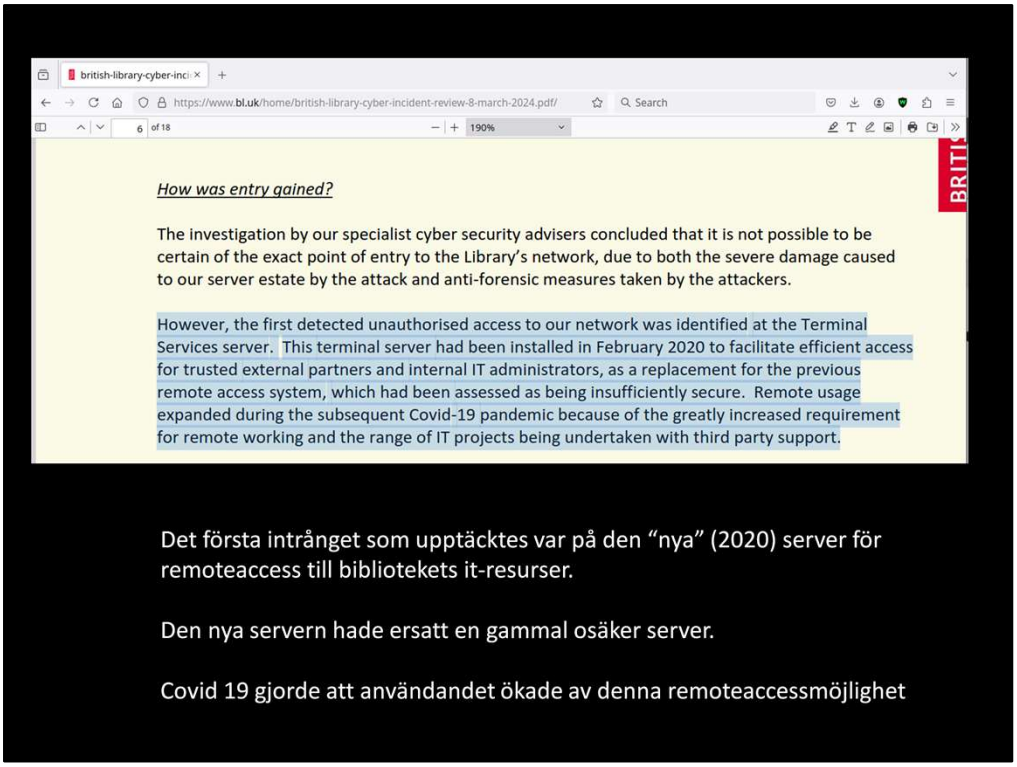
Kort sammanfattat så var det en cyberkriminell grupp rhysida som gjorde en så kallad ransomware-attack där de tog sig in laddade ned en massa data, krypterade systemen och förstörde därmed möjligheten att använda dom.

De krävde en lösensumma på 20BTC för att återställa tjänsterna. Biblioteket betalade inte och därmed släppte gruppen ca 600Gb data online.

En spekulation på nätet i och med att gruppen rhysida tillhandahåller "ransomware as a service" är att de valde just British library som mål i rent marknadsföringssyfte.

British library har gjort något så ovanligt att faktiskt ge ut en "lessons-learned"-skrift i mars i år.

Jag ska göra några nedslag i denna rapport.

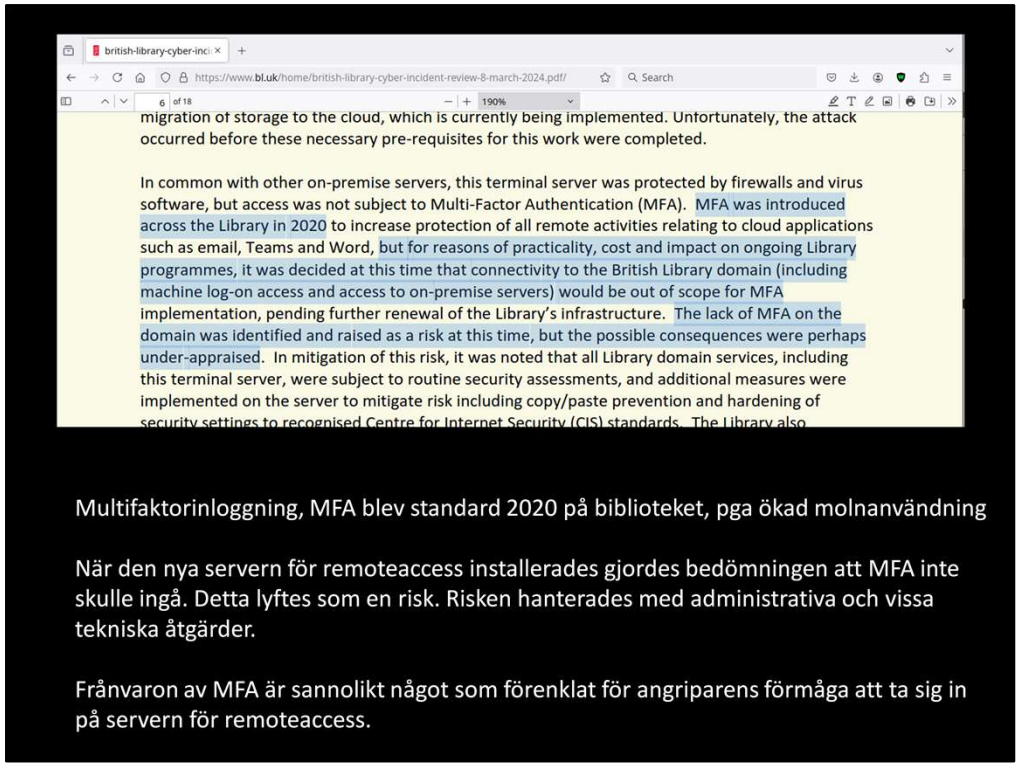


Hur tog dom sig in?

I beskrivningen så framgår att biblioteket har en tjänst som ger fjärråtkomst till bibliotekets IT-resurser.

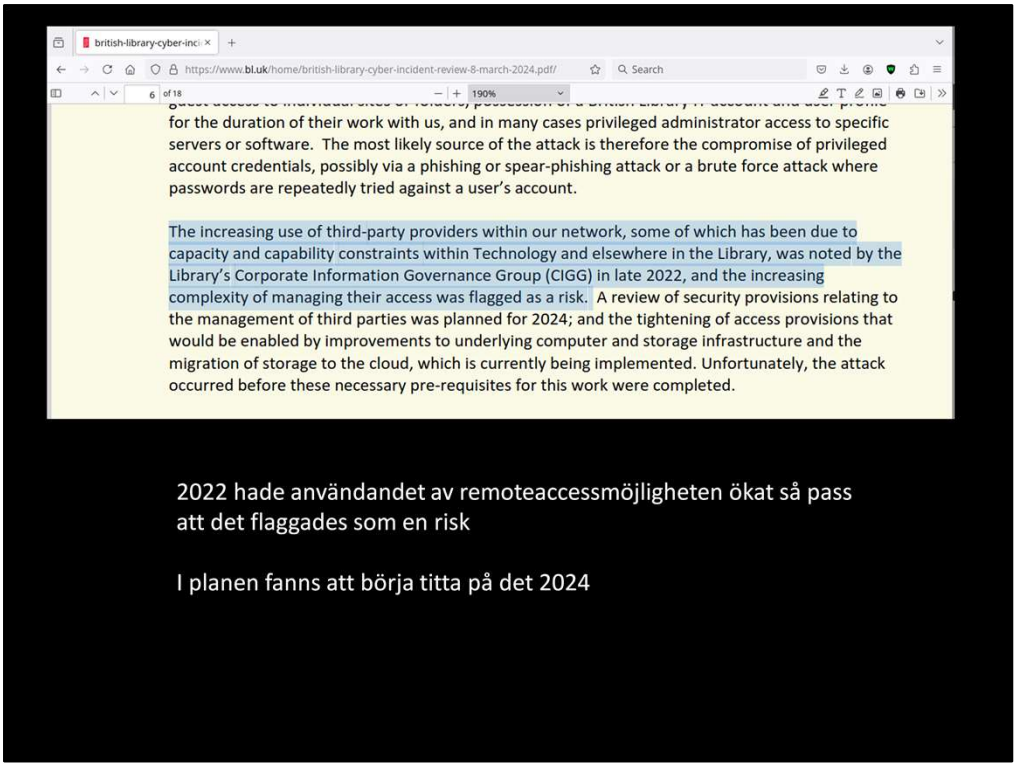
Denna tjänst moderniserades 2020 med en ny server för att den gamla ansågs osäker.

Rapporten drar slutsatsen att de förmodligen tog sig in via den nya server som moderniserats.



När den nya servern infördes så fanns det ett generellt krav på Multifaktorinloggning i bibliotekets regler, men av ett antal anledningar så bestämdes att just denna servern skulle undantas från kravet och istället gjordes ett antal alternativa åtgärder för att kompensera för detta av främst reaktiv karaktär (övervakning och granskning).

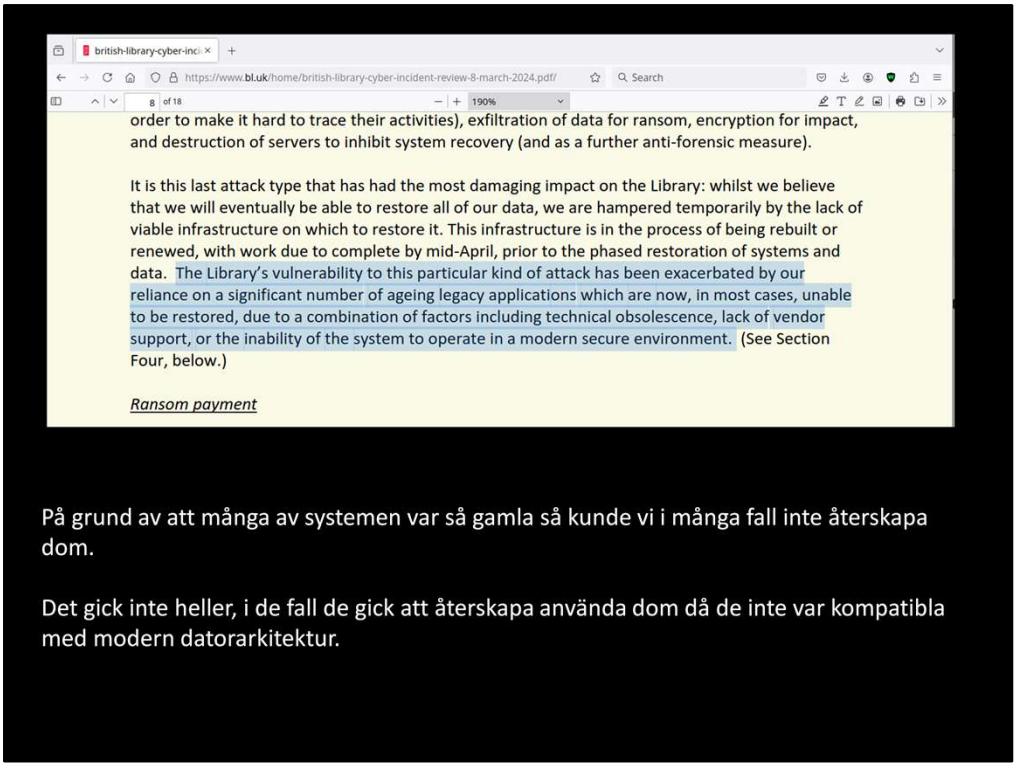
Frånvaron av MFA är sannolikt något som förenklat för angriparens förmåga att ta sig in via servern för remoteaccess.



Covidpandemin bidrog tilll att användandet fjärråtkomstmöjligheten blev större och mer långtgående än vad som ursprungligen planerats.

2022 noterades att användandet hade ökat så pass mycket att det flaggades som en risk.

Denna risk planerades att tas om hand 2024 i samband med att hela bibliotekets it-miljö skulle förbättras.



Några iakttagelser kring konsekvensen av intrånget när det kommer till återställning eller som det heter på IT-språk Disaster recovery.

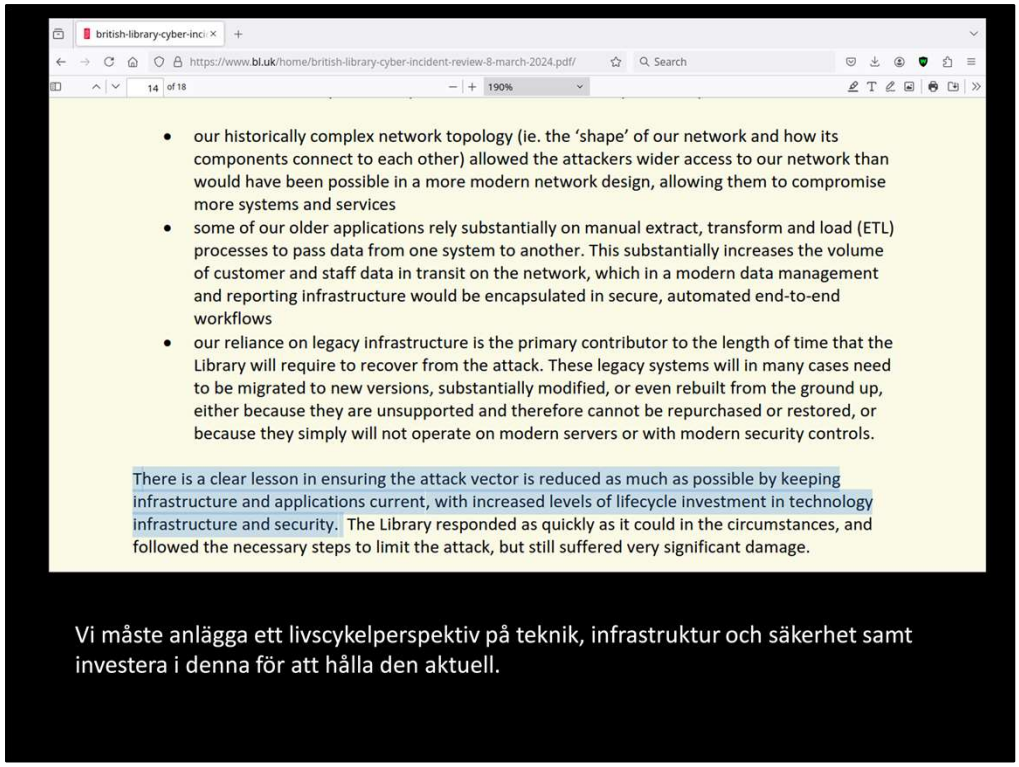
När det kommer till den värdebärande informationen så lyckades man förmodligen hitta backuper på all data, angriparna hade inte lyckats kryptera denna information.

Den största konsekvensen av attacken blev att återställning av själva IT-systemen försvårades.

Många system var helt enkelt så gamla att det inte fanns någon leverantör kvar eller att systemen inte var kompatibla med modern datorarkitektur.

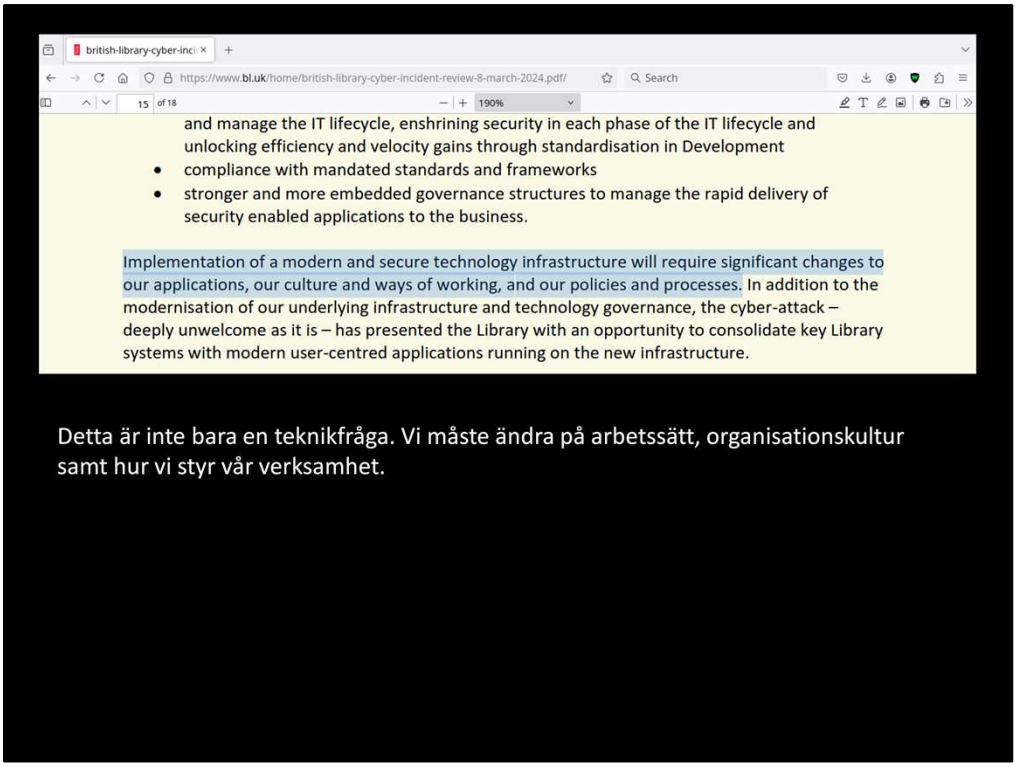
Så återställningsarbetet blev istället ett utvecklingsarbete av nya plattformar och system.

Det tar tid!



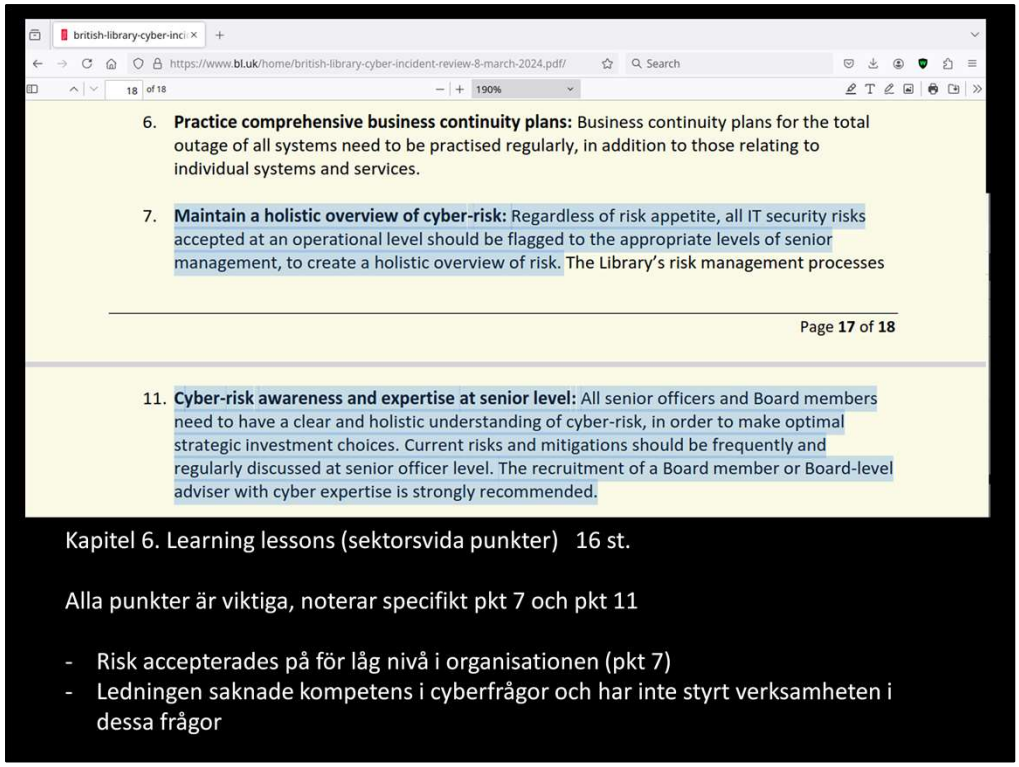
Vad för slutsatser har det dragits?

En slutsats biblioteket dragit är att de måste anlägga ett livscykelperspektiv på teknik, infrastruktur och säkerhet samt investera i denna för att hålla den aktuell.



En annan slutsats är att:

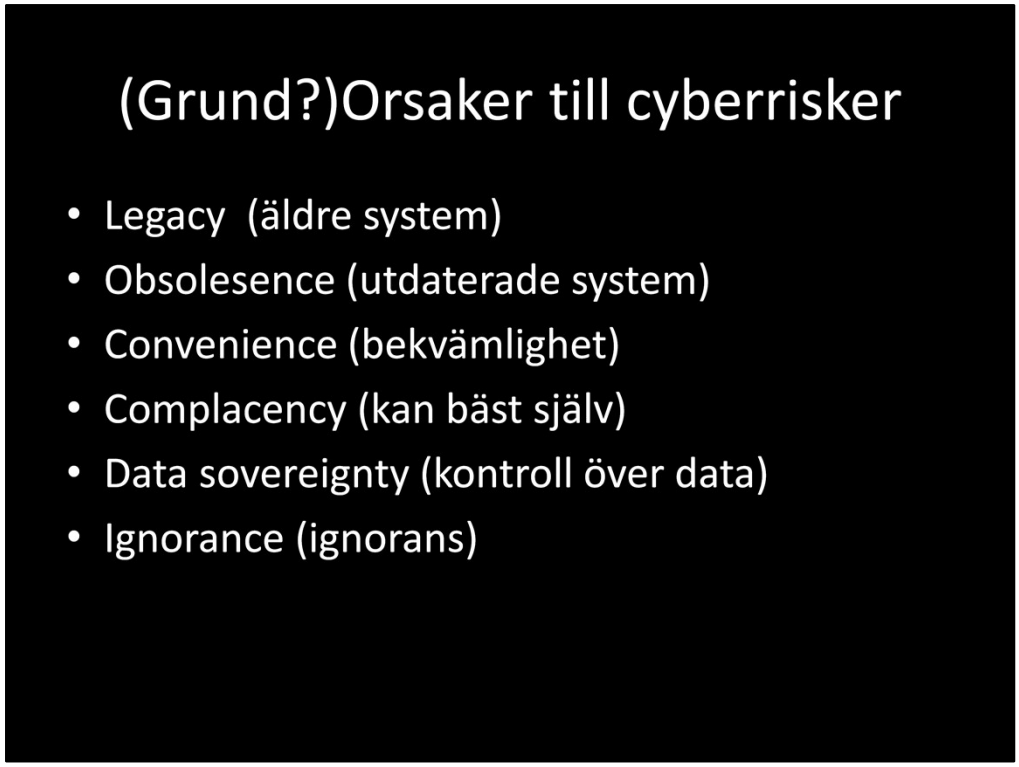
Detta inte bara är en teknikfråga. Vi måste ändra på arbetssätt, organisationskultur samt hur vi styr vår verksamhet.



Rapporten avslutas med ett "lärdomskapitel" med 16 punkter som alla är viktiga.

Jag vill specifikt lyfta fram två punkter (7 och 11 i rapporten), som jag sammanfattar med:

- Risk accepterades på för låg nivå i organisationen, dvs ledningen tog inte i dessa frågor på en högre nivå.
- Ledningen saknade kompetens i cyberfrågor och har inte kunnat styra verksamheten i detta avseende.



Så avslutningsvis vill jag skicka med några.

Grund? Orsaker till cyberrisker och tackar härmed återigen för förmånen att få tala inför denna församling.

Tack!

Kontaktuppgifter: jb@brandbergtechnology.se