Verklighetskuben: en analysmodell för att analysera cybersäkerhetsincidenter i totalförsvaret.

Mattias Svahn, Henrik Karlzén och Anders Melander

Att definiera något som en kris avslöjar att avgörandet ligger i betraktarens ögon, den är en social konstruktion. Händelsen måste bli socialt konstituerad mellan en rad aktörer. Om ingen reagerar på händelsen och uppfattar den som en kris, så är det heller ingen kris.[1]

När blir något en kris? Det inledande citatet pekar på att detta sällan är enkelt att avgöra. Det skrevs år 2000, i en helt annan kontext än dagens digitala samhälle, men citatet är möjligen ännu mer relevant idag. För att värdera en situation behöver vi först uppfatta den och ibland går uppfattningarna isär; ibland blåser vi upp något bortom dess proportioner och vid andra tillfällen missar vi helt en krissituation. Hur ska detta hanteras? Frågan om hur kris uppfattas är fokus i detta memo, som fokuserar på händelser i informationsmiljön.

1. Introduktion

Den digitala infrastrukturen är idag en grundförutsättning för centrala samhällsfunktioner.[2] Störningar i IT-system påverkar inte enbart teknisk funktionalitet. De påverkar också människors tolkning av störningarna i IT-systemen, vilket kan leda till ifrågasättande av om de är tillförlitliga, och i så fall påverkas tilliten till det digitala samhället. Cybersäkerhet bör därför förstås både som processen att skydda tekniska system och även som ett sociologiskt och ett psykologiskt fenomen.

I dessa sammanhang brukar man prata om att cybersäkerhet utspelar sig i den så kallade informationsmiljön.[3] Begreppet är ett sätt att förstå kopplingen mellan fysiska informationssystem, de sociala sammanhang inom vilka information sprids i medier och den kognitiva dimensionen, som finns i våra huvuden och där information tolkas och, ibland, omsätts i beteendeförändring. Det är de sociala och kognitiva dimensionerna som är av huvudsakligt intresse såväl för det psykologiska försvaret som för denna text, men de fysiska systemen utgör förstås också en nödvändig förutsättning för informationsmiljön.[4] Kort sagt kan man säga att informationsmiljön utgörs av de medier vi konsumerar, de samtal vi för och den tolkningsvärld som individer, eller grupper av individer, skapar tillsammans.

Informationsmiljön är emellertid komplex och människor som vistas i den är ständigt utsatta för ett bombardemang av information och olika tolkningsmöjligheter. Antagonistiska aktörer försöker därtill att sprida lögner, angripa informationssystem och utföra dataintrång på en daglig basis för att främja sina intressen.[5] Realtidsöverföring av information, parallella narrativ och konkurrerande verklighetsbeskrivningar skapar en komplex och potentiellt destabiliserande informationsmiljö.

Cybersäkerhet ska skydda mot cyberincidenter. När vi säger att cybersäkerhet också bör förstås som ett sociologiskt och psykologiskt fenomen, är det kanske bra att definiera vad vi menar med en cyberincident. En incident i cyberdomänen definieras enligt

1 Brändström, *Minkar eller ubåtar i den svenska ubåtsjakten,* sid. 10.

2 Digitaliseringsmyndigheten, *Mot ett digitalt Sverige 2030*.

3 Nilsson m.fl., *Den nya informationsmiljöns topografi - Teknik, människa och strategi i osäkerhetens tidevarv*; Floridi, *Information.a very short introduction*

4 Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE).*; Pamment och Isaksson, *Psychological Defence: Concepts and principles for the 2020s*; Porada och Lisník, ”Propaganda, Disinformation, Informational, Psychological and Mental Warfare as Instruments of Power in Globalized World”.

5 Monsees, ”Information disorder, fake news and the future of democracy”.

FOI Memo 9319
Projektnummer: A126703
Godkänd av: Sara Brunnberg

Maj 2026

NIS2-direktivet för cybersäkerhet[6] som ”en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem”. Fokus är alltså på vad som kan skada information och tjänster. Cyberincidenter och deras indikatorer kan delas in i fyra fall, utifrån två dimensioner: huruvida incidenten faktiskt har inträffat eller inte och huruvida den av bedömare uppfattas som verklig eller inte. I detta memo fokuserar vi främst på incidenter som märkbart har upplevts, till exempel falsklarm, missuppfattningar och liknande som ändå betraktats som verkliga. Vi går inte in på de incidenter som finns, men aldrig märks. I utredningar av cyberincidenter läggs ofta fokus på tekniska belägg. Det rör sig exempelvis om loggar, indikatorer på kompromettering eller andra forensiska bevis. Men upplevelsen av en incident är också viktig och kan uppstå även utan, eller med begränsade, tekniska belägg.

Ibland sker angrepp mot svenska aktörer som får stora effekter, som dataintrånget hos företaget Miljödata 2025.[7] Andra gånger sker stora dataintrång eller desinformationsangrepp utan att någon märker det, och ibland får egentligen ganska oväsentliga incidenter stor uppmärksamhet[8], vilket är det som skapar omfattande psykologiska effekter.

Vad händer till exempel när folk slutar lita på samhällsviktiga digitala tjänster som exempelvis bank-ID eller betaltjänsten Swish? Eller vad händer när viktiga databaser i offentlig sektor slutar fungera och orsaken till det är oklar? Hur kan lekmän avgöra när det är dags att slå larm, och när det kanske inte är det?[9]

I detta memo presenteras en modell för att skapa förståelse kring detta. Vi kallar den ”Verklighetskuben”. Verklighetskuben är tänkt att ge lekmän möjlighet att bedöma gränslandet mellan det verkliga och det upplevda. Den ska ge icke-tekniska personer ett verktyg att använda när samhällsviktiga digitala tjänster som bank-ID och Swish eller databasen på jobbet slutar (eller verkar sluta) fungera och vi inte förstår varför.

2. Verklighetskuben: en analysmodell för totalförsvaret

Verklighetskuben är ett analysverktyg framförallt tänkt att hantera cybersäkerhetsincidenter i totalförsvaret, men vilket kan användas för att beskriva osäkra situationer i allmänhet på ett strukturerat sätt. Modellen möjliggör systematisk bedömning av när förståelsen krackelerar och när totalförsvarets aktörer kanske kan komma att agera på oklar grund. För att analysera hur händelser inom informationsmiljön, särskilt cyberrelaterade sådana, påverkar aktörer inom det civila och psykologiska totalförsvaret utgår modellen från tre glidande skalor: graden av upplevd kunskap om en händelse (kubens X-axel), graden av hur verklig en händelse upplevs vara (kubens Y-axel) och graden av institutionella åtgärder utifrån dessa två (kubens Z-axel).

2.1 Grad av upplevelse av kunskap (x-axeln)

X-axeln representerar graden av teknisk verifierbarhet, det vill säga hur starkt tillgängliga tekniska bevis stödjer en händelse. Axeln fångar kunskapsstatus och tillgången till sådan teknisk validering som uppfattas relevant i en situation. Ett högt värde på denna axel innebär att händelsen bedöms som tydligt verifierad genom t.ex. loggar eller systempåverkan. Ett lågt värde på axeln innebär att förståelsen bygger på spekulation, vaga indikationer eller uppfattningar med oklar teknisk grund. Olika yrkesgrupper kan ha olika uppfattningar om detta. Exempelvis kan teknisk personal utgå från nätverksdata, medan beslutsfattare relaterar till rapporter om systempåverkan eller vad som går att läsa i tidigare beredskapsplaner. Vad som räknas som goda bevis kan alltså variera mellan aktörer.[10] Det handlar inte om sanning i absolut mening utan om upplevd grad av underlag för att bedöma en cybersäkerhetssituation.

2.2 Grad av upplevelse av verklighet (y-axeln)

Y-axeln visar i vilken grad en händelse uppfattas som verklig inom de institutionella och sociala tolkningsramarna. Y-axeln i modellen avser den verklighetsstatus en cyberincident får, det vill säga i vilken grad en incident uppfattas som verklig, misstänkt, tveksam eller rentav som en illusion. Det som definieras som verkligt

6 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (Text av betydelse för EES).

7 IMY, ”Integritetsskyddsmyndigheten | IMY”.

8 Collier, ”A “Sophisticated Attack”? Innovation, Technical Sophistication, and Creativity in the Cybercrime Ecosystem”.

9 Boholm, ”Twenty-five years of cyber threats in the news”.

10 Såsom beskrivet i bl.a. Floridi, ”The Method of Levels of Abstraction”.

(Y) är ofta, men inte alltid, en funktion av vilken kunskap aktörer upplever sig ha (X). För modellens syfte gör vi en analytisk åtskillnad: Y-axeln avser upplevelsen av verklighet, medan X-axeln behandlar upplevelsen av kunskap. Dessa dimensioner samverkar ofta, men vi vill förtydliga att det ändå representerar olika tolkningar i aktörernas förståelse av en cyberincident. Det som skiljer Y från X är att vi kan tro att en cyberincident är verklig (Y) även med lite underlag för det (låg X), eller tro att cyberincidenten är overklig (Y) med mycket underlag för det (hög X). Dessa två axlar ger då fyra olika kombinationer av upplevelser.

I praktiken manifesteras detta i hur organisationer i totalförsvaret reagerar på rykten eller preliminära rapporter: en informationsläcka eller driftstörning som snabbt får spridning i nyhetsmedier eller sociala medier kan uppfattas som verklig (hög Y) trots att tekniska bevis ännu kanske inte är på plats (låg X), och därmed ändå föranleda åtgärd. Omvänt kan en tekniskt verifierad incident (hög X) initialt avfärdas eller tonas ned om den inte passar in i aktörens tolkningsram eller erfarenhet (låg Y). Här kan det uppstå ett glapp mellan upplevd verklighet (Y) och faktisk kunskap om verkligheten (X) - ett glapp som Verklighetskuben synliggör.

2.3 Grad av åtgärd (z-axeln)

Den tredje dimensionen är Z-axeln, den fångar den institutionella responsens omfattning: vad gör aktörer i totalförsvaret utifrån upplevelserna uttryckta på X- och Y-axlarna. Vilka policybeslut fattas? Vilka resurser aktiveras? I Z-ledet rör det sig om hur starkt en händelse i samhället leder till åtgärder. Detta är inte nödvändigtvis bara kopplat till teknisk grund eller upplevd verklighet av cyberincidenter. Det är möjligt att samhälleliga åtgärder kan aktiveras även med lite underlag (X) och även om det är oklart vad som är verkligt (Y), om det är viktigt på grund av bredare narrativ, förväntningar eller institutioners policy. Att få sådan uppmärksamhet och åstadkomma en sådan reaktion kan vara ett mål för en antagonistisk aktör.[11] Z-axeln representerar graden av åtgärd. En incident som triggar myndighetsinsatser, krismöten eller policyförändringar har därför ett högt Z-värde. Ett lågt Z-värde innebär istället att graden av åtgärd varit liten, även om det rör en väl underbyggd incident (X) som är verklig (Y).

2.4 Alla platser i ”verkligheten”

Om vi tänker oss att var och en av de tre axlarna är en tänkt skala från låg till hög och vi för enkelhetens skull tänker oss tre lägen på varje axel, låg, hög och medel, till exempel som en lite mindre Rubiks kub med formatet 3×3×3, då kan var och en av de tre positionerna på X-axeln kombineras med tre olika positioner på Y och för varje sådan kombination finns det sedan tre var på Z. Det ger 32 = 9 möjliga lägen för varje X. Eftersom det finns tre X-positioner blir det totalt 33 = 27 möjliga kombinationer i hela Verklighetskuben. Liksom vi kan vrida på en Rubiks kub och få fram många olika kombinationer, får vi med denna utgångspunkt 27 olika mått på hur en cyberincident kan förstås och upplevas.

Det är värt att lyfta fram att var och av de 27 olika platserna i kuben kan leda till olika konsekvenser. När ledare inom totalförsvaret vidtar omfattande åtgärder (hög Z) på begränsat tekniskt underlag (låg X) och med en osäker uppfattning om händelsens verklighet (låg Y), ökar risken för åtgärder som inte är optimalt anpassade till situationen. På samma sätt kan medborgarnas förtroende urholkas om stora åtgärder vidtas (Z) utan att det är tydligt vilken kunskap (X) eller vilken verklighetsbedömning (Y) som ligger till grund för dem

2.5 Förståelsekris och förståelseresiliens

Dilemmat kan sammanfattas i två begrepp. Förståelsekris inträffar när aktörer har svårt att skilja mellan fakta, sin egen tolkning och fiktion. Det leder till överreaktion, handlingsförlamning eller strategisk desorientering. Förståelseresiliens är förmågan att upprätthålla omdömesförmåga och handlingskapacitet även i lägen av förståelsekris.

Med hjälp av Verklighetskuben kan vi formulera en analytisk hypotes kopplad till dessa begrepp. Begreppen blir därmed inte bara beskrivande i efterhand, utan också möjliga att använda för att i förväg identifiera situationer där sådana tillstånd kan uppstå. Hypotesen är att förståelsekris tenderar att uppkomma i scenarier där graden av kunskap (X) är låg, upplevelsen av verklighet (Y) är hög och kraven på grad av åtgärd (Z) samtidigt är hög, med andra ord när aktörer känner sig pressade att agera snabbt och kraftfullt på en cyberincident i ett läge där agerandet fortfarande har oklar teknisk grund (X).[12]

Förståelseresiliens kännetecknas istället av att det finns en samverkan mellan de tre dimensionerna till exempel

11 Giannopoulos, m.fl., *The Landscape of Hybrid Threats: A Conceptual Model Public Version*.

12 För att stryka under det, är det värt att nämna att forskning visar på att det kan finnas en mediadynamik och säkerhetspolitisk dynamik som skapar incitament för att skildra en cyberattack som mer sofistikerad än den egentligen var t.ex. Collier, ”*A “Sophisticated Attack? Innovation, Technical Sophistication, and Creativity in the Cybercrime Ecosystem”;* .

när tekniskt underlag (X), upplevd verklighet (Y) och åtgärd (Z) är samordnade, eller där en organisation har förmåga att fatta rimliga beslut även när underlaget är osäkert eller motsägelsefullt, kanske för att de har tid att ta fram ett ordentligt underlag (X+Z).

3. Fallstudier i lägen av ovisshet

För att illustrera detta kanske något abstrakta resonemang beskrivs här några exempel där samhällsinstitutioner har befunnit sig i antingen en förståelsekris, eller visat förståelseresiliens.

Fallstudierna kan också ses som praktiska prövningar av de hypoteser som föregående avsnitt formulerade kring förståelsekris och förståelseresiliens. Genom att placera varje händelse längs de tre axlarna i Verklighetskuben, upplevd kunskap (X), upplevd verklighet (Y) och grad av åtgärd (Z) kan vi analysera vilka mönster som återkommer. När exempelvis åtgärder vidtas på svagt underlag i ett läge som ändå upplevs som verkligt, stärks hypotesen om att förståelsekris är ett troligt utfall. Motsatsen: när kunskap, verklighetsuppfattning och insats ligger i fas, tyder det på förståelseresiliens.

Först ett tänkt exempel: Jag upplever att Swish inte fungerar. Beror det på ett tekniskt fel i min egen telefon (lokalt problem), är det ett driftsfel hos banken på grund av en bugg, eller är det en riktad cyberattack från en antagonist? När min kunskapsnivå (X) är låg men min upplevelse av verklighet (Y) ändå är hög, kan mitt agerande (Z) att exempelvis på sociala medier skriva ”Vad är det som händer med Swish?” i sig bidra till viral spridning och leda till ökad osäkerhet i samhället. Nu följer några exempel från situationer som faktiskt har hänt. Dessa exempel är valda för att illustrera modellen genom att belysa en variation längs alla tre axlarna. Exemplens placering i verklighetskuben syns i figur 1.

Oracle och misstänkta dataläckor (2025)

Våren 2025 spreds rykten om att angripare kanske hade fått tillgång till känslig information genom Oracles molntjänster. Trots frånvaro av teknisk verifiering utfärdade den amerikanska cybersäkerhetsmyndigheten CISA varningar.[13] Händelsen är en situation där upplevelsen av kunskap var oklar (X) eftersom det inte gick att tekniskt fastställa någon faktisk incident. Upplevelsen av verklighet (Y) var låg, inte för att dataläckan inte existerade, utan för att aktörer ännu inte tillskrev den verklighetsstatus, vilket i sin tur berodde på låg teknisk verifierbarhet (X). Likväl visar de publicerade varningarna att det fanns en grad av åtgärd (Z). Detta visar hur tillgång till data och tolkningens grad av säkerhet ofta samverkar i praktiken, även om de skiljs analytiskt i modellen. Graden av åtgärd (Z) kan i detta fall ses som medelhög med tanke på utfärdade varningar. Fallet illustrerar hur blotta uppfattningen av ett hot kan aktivera rutiner. Här kan vi se ett exempel på förståelsekris.

Google Maps och simulerad trafikstockning (2020)

I början av 2020 rapporterades det om ett konstnärligt experiment där en person i Berlin hade lagt ungefär hundra smartphones i en handdragen vagn och drog den på gatorna i Berlin. Detta simulerade en trafikstockning i Google Maps.[14] Trots att inga fordon faktiskt stod stilla, registrerade den välkända kartappen en trafikstockning vilket reellt påverkade andra trafikanters vägval. Incidenten skapade en illusion i informationsmiljön vilket gav upphov till ett narrativ om trafikstockning och därmed faktisk effekt i form av ändrade körvägar. Upplevelsen av kunskap (X) var låg eftersom få visste att det ”bara” var en konstnärlig händelse. Det kanske går att säga att den var hög, eftersom Google Maps tydligt visade en trafikstockning, men det var alltså ändå utan riktigt underlag. Trafikstockningen existerade endast i informationsmiljön, inte i den verkliga verkligheten. Det leder till att vi får klassa upplevelsen av verklighet (Y) som medelhög eftersom många, baserat på den vanligtvis trovärdiga Google Maps, faktiskt trodde att det fanns en trafikstockning. Åtgärder (Z) uteblev eftersom ingen institutionell aktör i Tyskland eller någon annanstans aktiverade motåtgärder. Detta kan kallas för ett rätt milt exempel på förståelsekris.

Kalix kommun och utpressningsvirus (2021)

I december 2021 drabbades Kalix kommun av ett angrepp med utpressningsvirus som slog ut centrala IT-funktioner inom kommunal förvaltning.[15] Upplevelsen av kunskap *(X)* var hög, det fanns gott om underlag med tydliga tekniska spår av intrång och kryptering. Det var ingen tvekan om att det var verkligt (Y), eftersom händelsen resulterade i högst observerbara och institutionellt bekräftade konsekvenser inom till exempel äldreomsorgen. Detta avspeglar inte bara en högre grad av existens i sig, utan också en stark aktörsgemensam uppfattning om att incidenten faktiskt var reell.

13 CISA, ”CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise | CISA”.

14 Hern, ”Berlin Artist Uses 99 Phones to Trick Google into Traffic Jam Alert”.

15 Kalix Kommun, *Rapport IT-attacken socialförvaltningen Kalix kommun.*; Kalix, ”Kalix hantering av IT-attacken gav eko i hela världen”.

Åtgärderna (Z) skedde till större delen på kommunal nivå, men beslut från Myndigheten för samhällsskydd och beredskap, MSB, att ta fram och publicera en rapport[16] innebar ändå ett visst mått av nationell uppföljning. Det gör att platsen på Z-axeln kan bedömas som medelhög. Åtgärderna var inte enbart lokala, men heller inte av sådan omfattning att de nådde upp till ett högt Z-värde. Utifrån definitionen i det här kapitlet och de angivna värdena för Verklighetskuben, innebär detta ett exempel på förståelseresiliens.

Crowdstrike (2024)

Sommaren 2024 drabbades stora delar av världen av omfattande IT-störningar efter en felaktig uppdatering i säkerhetsprogramvaran CrowdStrike Falcon för Windows-system. Enligt CISA berodde avbrotten på en programuppdatering som orsakade systemkrascher, inte på ett antagonistiskt cyberangrepp.[17] Samtidigt var effekterna i vardagen mycket påtagliga. Flygplatser, kollektivtrafik, vård och andra verksamheter rapporterade störningar i incheckningssystem, biljettförsäljning och administrativa system, något som bland annat rapporterades av SVT.[18]

I termer av Verklighetskuben innebar detta att upplevelsen av verklighet (Y) snabbt blev hög. Människor såg konkret att tjänster slutade fungera och media rapporterade om ett globalt IT-haveri. Däremot var upplevelsen av kunskap (X) initialt blandad. Det tog tid innan myndigheter och företag nådde en tydlig, gemensam bild av orsaken, och under denna period cirkulerade olika hypoteser och rykten. Åtgärdsgraden (Z) var däremot hög. Myndigheter som USA:s cybersäkerhetsmyndighet CISA gick ut med varningar.[19] Stora organisationer stängde ned system, och tekniker världen över arbetade intensivt med att återställa drabbade datorer.

Parallellt utnyttjades incidenten i både cyberbrottslighet och informationspåverkan. Cybersäkerhetsföretaget McAfee beskriver hur bedrägeriförsök knöts till händelsen.[20] Även EUvsDisinfo dokumenterade hur Rysslandsvänliga kanaler försökte väva in CrowdStrike-haveriet i längre narrativ om den så kallade Russiagate-affären.[21] På så vis illustrerar incidenten hur hög Y och hög Z kan samexistera med en initialt osäker X-nivå och hur den osäkerheten snabbt fylls av både krishanterande åtgärder och antagonistiska narrativ. Fallet visar hur rykten kan ge bild av att en cyberincident är ett antagonistiskt hot oavsett om det verkligen är det eller inte. Här kan vi se ett exempel på förståelsekris, i alla fall initialt.

KA-SAT-incidenten vid invasionen av Ukraina (2022)

Samma dag som Rysslands fullskaliga invasion av Ukraina inleddes i februari 2022, rapporterades omfattande driftstörning i Viasats KA-SAT-satellitnätverk.[22] Många satellitmodem slogs ut, främst i Europa inklusive i Ukraina där både civila och militära kommunikationssystem påverkades.[23] Händelsen betraktades snabbt som möjlig förberedelse för invasionen. Viasat själva var återhållsamma med information om intrånget och den tekniska bakgrunden förblev länge oklar.[24] Både EU och Storbritannien skyllde offentligt på Ryssland, trots begränsad teknisk bevisning.[25] Initialt var det stor ovisshet (X) eftersom teknikexperter och media hade mycket begränsad insyn. Det var osäkert vad som var verkligt (Y), då det fanns osäkerhet om vad som egentligen pågick. Detta påverkade hur verklig incidenten uppfattades som. Exempelvis noterade många användare endast att uppkoppling saknades.[26] Det fanns en tydlig grad av åtgärd (Z). Västerländska regeringar fördömde attacken och integrerade den i större narrativ om rysk hybridkrigföring samt införde sanktioner. Här kan vi se ett till exempel på förståelsekris.

16 MSB, *Cyberangrepp mot samhällsviktiga informationssystem 25 rekommendationer för stärkt skydd mot cyberangrepp*.

17 CISA, ”Widespread IT Outage Due to CrowdStrike Update | CISA”.

18 Wickström och Wiman, ”Grundproblemet löst efter globala it-störningar”.

19 CISA, ”Widespread IT Outage Due to CrowdStrike Update | CISA”.

20 Mathur m.fl., ”The Scam Strikes Back”.

21 EU vs Disinfo, ”Disinfo”.

22 Viasat, ”KA-SAT Network Cyber Attack Overview”.

23 EuRepoC, ”Major Cyber Incident”.

24 Cyberpeace Institute, ”Case Study”.

25 EuRepoC, ”Major Cyber Incident”; Cyberpeace Institute, ”Case Study”.

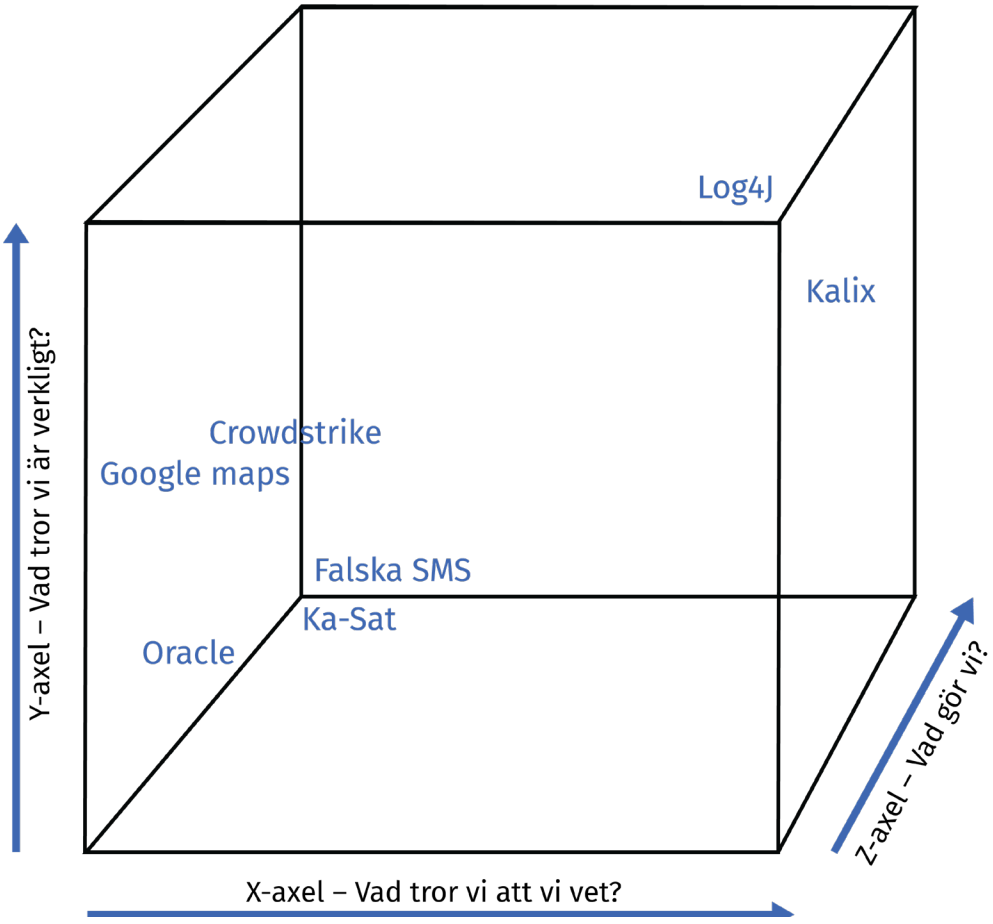
26 Pearson, ”Russia Downed Satellite Internet in Ukraine -Western Officials”.

Log4j-sårbarheten Log4Shell (2021)

I december 2021 upptäcktes en allvarlig sårbarhet i Java-biblioteket Log4j, som används globalt i miljontals servrar och system.[27] Sårbarheten (Log4Shell) möjliggjorde för angripare att fjärrköra kod på sårbara system. Sårbarheten klassades snabbt som allvarlig[28] och cybersäkerhetsmyndigheter världen över utfärdade varningar[29]. Många organisationer svarade dock långsamt, uppdaterade inte i tid, och hade begränsad förmåga att ens identifiera om de var sårbara. Tekniska detaljer och exempel på utnyttjanden blev snabbt kända, så upplevelsen av kunskap (X) var hög. I fråga om att se hotet som verkligt (Y) är dock bedömningen mer ambivalent. Det fanns en konkret sårbarhet med tydliga angreppsvektorer. Graden av åtgärd (Z) varierade dock mellan enskilda myndigheter, kommuner och företag. Här kan vi se ett exempel på förståelsekris. Även om cybersäkerhetssårbarheten var allvarlig så var många parter inte så uppmärksamma på att se den som ett hot mot den just den egna organisationen.

Falska SMS om väpnat angrepp (2025)

I september 2025 mottog flera personer i västra Sverige ett falskt SMS där det felaktigt påstods att Sverige hade utsatts för ett väpnat angrepp och att regeringen beslutat om ”höjd krigsberedskap”.[30] Meddelandet påstods komma från SOS Alarm och dök i vissa fall upp i samma SMS-meddelandetråd som tidigare autentiska varningar, vilket gav det trovärdighet. Händelsen väckte oro och ledde till att polis, medier och SOS Alarm snabbt gick ut



Figur 1. Verklighetskuben.

27 CISA, ”Apache Log4j Vulnerability Guidance | CISA”.

28 NCSC UK, ”Log4j Vulnerability - What Everyone Needs to Know”.

29 CISA, ”Mitigating Log4Shell and Other Log4j-Related Vulnerabilities | CISA”.

30 SOS Alarm, ”Information med anledning av falska sms - SOS Alarm”; Nyheter, ”Falska sms sprids påstås att Sverige utsätts för väpnat angrepp”.

med korrigerande information.[31] Polisen utredde det som grovt falsklarm eller föregivande av allmän ställning.[32] Det fanns ovisshet om graden av kunskap, det vill säga meddelandets autenticitet (X). Vissa mottagare trodde på att något allvarligt inträffat, medan andra snabbt avfärdade det. I fråga om att se det som verkligt (Y) förelåg instabilitet eftersom utskicket förändrade informationsmiljön trots att inget faktiskt hot förelåg. Graden av åtgärd (Z) var hög, snabb och tydlig.

4. Verklighetskubens applicering

Vi har i detta memo presenterat Verklighetskuben som ett analysverktyg för att förstå samspelet mellan tekniskt underlag, upplevd verklighet och grad av åtgärd vid störningar i samhället som uppstår i eller genom informationsmiljön. Modellen syftar till att identifiera och analysera lägen där olika aktörer, från enskilda personer till myndigheter och företag på olika sätt upplever och reagerar på händelser i digitala miljöer utifrån skilda tolkningar och kunskapsunderlag.

I Försvarsmaktens militärstrategiska doktrin (MSD 22) betonas att nationell säkerhet i allt högre grad vilar på digitala grunder. I detta ligger inte bara behovet av teknisk robusthet, utan också förmågan att uppfatta, tolka och hantera situationer där informationsflöden skapar osäkerhet, motsägelsefulla bilder eller narrativt drivna uppfattningar. Tidigare forskning använder många olika begreppsapparater. Med Verklighetskuben har vi en ny modell som översätter de olika begreppsapparaterna till ett konkret och tillämpbart analysverktyg.

Modellen visar hur dessa tre dimensioner inte bara samverkar utan även ibland divergerar. En händelse kan exempelvis uppfattas som verklig utan att tekniskt kunna beläggas, vilket i vissa fall ändå kan leda till omfattande åtgärder i totalförsvaret. Eller omvänt att en tekniskt bekräftad händelse, som inte tolkas som allvarlig, kan leda till uteblivna insatser. Det är just i dessa diskrepanser som det vi här kallar för en förståelsekris kan uppstå, ett tillstånd där aktörernas förmåga att särskilja mellan fakta, tolkning och fiktion kollapsar och riskerar att försvaga samhällets förmåga att fatta kloka beslut under osäkerhet. Mot detta står begreppet förståelseresiliens, det vill säga förmågan att upprätthålla gott omdöme och handlingsförmåga trots oklara underlag, motsägelsefull information och hög press. Modellen gör det möjligt att identifiera dessa lägen i förväg, spåra var i organisationen bristande förståelse uppstår och var åtgärder riskerar att bli symboliska, otillräckliga eller överdrivna.

Genom att analysera sådana mönster över tid kan Verklighetskuben användas även i förebyggande syfte. Om en organisation exempelvis börjar kommunicera kraftfulla åtgärder i ett skede där teknisk verifiering ännu saknas och tolkningarna av händelsen spretar, kan detta tolkas som en indikation på att en förståelsekris håller på att utvecklas. Modellen kan då användas som beslutsstöd i realtid, och inte bara för efterhandsanalys, genom att uppmärksamma när X, Y och Z divergerar kraftigt. Det öppnar för en mer reflexiv beredskap, där det kan finnas medvetenhet om narrativ och där intern analys kan hinna ske innan åtgärder måste sättas in. Det innebär helt enkelt att tänka efter före.

Fallstudierna i föregående avsnitt har illustrerat hur aktörer befinner sig i olika positioner i denna kub, ibland med god teknisk grund men låg tolkad verklighet (som exemplet Oracle 2025), ibland i ett scenario där perceptionen av en händelse överträffar dess tekniska belägg (som exemplet Google Maps). Kalix kommun illustrerade i sin tur ett exempel på förståelseresiliens, där både verklighetsuppfattning, tekniskt underlag och insats låg i linje med varandra.

Genom att systematiskt analysera incidenter utifrån Verklighetskuben kan totalförsvarets aktörer förbättra förmågan till situationsförståelse och kontroll över samhällets narrativ. Det är en modell som ger stöd för beslut under osäkerhet, planering av kommunikation samt analys av operativ och strategisk respons. Sammantaget visar detta memo hur teoretiska begrepp som begreppet informationsmiljö kan vidareutvecklas till en mer konkret och handfast tillämpning i analysen av samhällets informationsrelaterade motståndskraft. Verklighetskuben erbjuder därmed ett metodiskt stöd för aktörer inom det civila och psykologiska försvaret i en tid där kampen om förståelse av en cyberincident i sig blivit ett strategiskt mål.

Det finns även andra fall utanför cybersäkerhetsmiljön där svårbedömda observationer med oklar verklighetsgrad ändå har skapat omfattande institutionella aktiveringar. Några exempel är ubåtsobservationerna i Sverige under 1980-talet[33], drönarobservationerna vid

31 SOS Alarm, ”Information med anledning av falska sms - SOS Alarm”; Nyheter, ”Falska sms sprids påstås att Sverige utsätts för väpnat angrepp”.

32 Nyheter, ”Falska sms sprids – påstås att Sverige utsätts för väpnat angrepp”.

33 Ekeus m.fl., *SOU (2001). Ubåtsfrågan 1981 1994: Rapport från 2001 års ubåtsutredning*; Brändström, *Minkar eller ubåtar i den svenska ubåtsjakten*.

kärnkraftverk och flygplatser 2022–2025[34] eller skadorna på undervattenskablar i Östersjön 2024–2025[35].

Verklighetskuben kan därmed fungera som ett strukturerande verktyg vid planering av övningar, analys av incidenter och utveckling av policy inom det civila och psykologiska försvaret. Genom att tydliggöra skillnader mellan faktisk kunskap, upplevd verklighet och institutionell respons kan modellen bidra till ökad förmåga att fatta beslut under osäkerhet, och förbättra aktörers förståelseresiliens över tid.

Modellen väcker även tankar för vidare analys: I vilka lägen uppstår förståelsekris särskilt lätt, och varför då? Hur kan förståelseresiliens tränas, inte bara som kognitiv förmåga hos en individ utan även som organisatorisk beteende? Vad händer när olika aktörer i totalförsvaret tolkar en cyberincident utifrån skilda placeringar i Verklighetskuben, hur påverkar det samordning och förtroende? Sådana frågor pekar på att modellen inte bara erbjuder en beskrivning av enskilda fall, utan också ett ramverk för strategisk dialog och lärande inom totalförsvarets civila och psykologiska delar.

34 Nyheter, ”Filmer visar drönarna över svenska kärnkraftverk”; SÄPO, ”Förundersökning tas över kring drönare vid kärnkraftverk”.

35 Nyheter, ”Detta vet vi”.

Referenser

Boholm, Max. ”Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019)”. Journal of Cybersecurity 7, nr 1 (2021): tyab016. https://doi.org/10.1093/cybsec/tyab016.

Brändström, Annika. Minkar eller ubåtar i den svenska ubåtsjakten. Ny utg. Försvarshögskolan, 2003.

CISA. ”Apache Log4j Vulnerability Guidance | CISA”. 08 april 2022. https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance.

CISA. ”CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise | CISA”. CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise, 16 april 2025. https://www.cisa.gov/news-events/alerts/2025/04/16/cisa-releases-guidance-credential-risks-associated-potential-legacy-oracle-cloud-compromise.

CISA. ”Mitigating Log4Shell and Other Log4j-Related Vulnerabilities | CISA”. 23 december 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a.

CISA. ”Widespread IT Outage Due to CrowdStrike Update | CISA”. Widespread IT Outage Due to CrowdStrike Update, 06 augusti 2024. https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update.

Collier, Ben. ”A “Sophisticated Attack”? Innovation, Technical Sophistication, and Creativity in the Cybercrime Ecosystem”. Conference paper presented vid 21st Workshop on the Economics of Information., Tulsa. 2022. https://weis2022.econinfosec.org/wp-content/uploads/sites/10/2022/06/weis22-collier.pdf.

Cyberpeace Institute. ”Case Study: Viasat Attack | CyberPeace Institute”. 2022. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

Digitaliseringsmyndigheten. Mot ett digitalt Sverige 2030. Dnr. 2024–1332. Digitaliseringsmyndigheten, 2024. https://www.digg.se/download/18.129a4fef1939e2e1c1f246c9/1709290044712/Mot%20ett%20digitalt%20Sverige%202030.pdf.

Ekeus, Rolf, Mathias Mossberg, och Birgitta Arvidsson. SOU (2001). Ubåtsfrågan 1981–1994: Rapport från 2001 års ubåtsutredning. Fritzes, 2001. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2001/11/sou-200185/.

EU vs Disinfo. ”Firm behind Global IT Outage Was Part of the Russiagate Hoax”. Firm behind Global IT Outage Was Part of the Russiagate Hoax, 2024. https://euvsdisinfo.eu/report/firm-behind-global-it-outage-was-part-of-the-russiagate-hoax/.

EuRepoC. ”Major Cyber Incident: KA-SAT 9A”. EuRepoC: European Repository of Cyber Incidents, u.å. Åtkomstdatum 08 oktober 2025. https://eurepoc.eu/publication/major-cyber-incident-ka-sat-9a/.

Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (Text av betydelse för EES), OJ L (2022). http://data.europa.eu/eli/dir/2022/2555/oj/swe.

Floridi, Luciano. Information: A Very Short Introduction. OUP Oxford, 2010.

Floridi, Luciano. ”The Method of Levels of Abstraction”. Minds and Machines 18, nr 3 (2008): 303–29. https://doi.org/10.1007/s11023-008-9113-7.

Giannopoulos, Giorgios, H Smith, och M Theocharidou. The Landscape of Hybrid Threats: A Conceptual Model Public Version. White Paper EUR 30585 EN. Hybrid CoE, 2021. https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

Hern, Alex. ”Berlin Artist Uses 99 Phones to Trick Google into Traffic Jam Alert”. Technology. The Guardian, 03 februari 2020. https://www.theguardian.com/technology/2020/feb/03/berlin-artist-uses-99-phones-trick-google-maps-traffic-jam-alert.

IMY. ”Integritetsskyddsmyndigheten | IMY”. Har personuppgifter om dig läckt i it-angreppet mot Miljödata?, 2025. https://www.imy.se/nyheter/har-personuppgifter-om-dig-lackt-i-it-angreppet-mot-miljodata/.

Joint Chiefs of Staff. Joint Concept for Operating in the Information Environment (JCOIE). JCS JCOIE 20180625. U.S. Department of Defense, Joint Chiefs of Staff, u.å. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

Kalix. ”Kalix hantering av IT-attacken gav eko i hela världen”. Kalix Kommuns hemsida, maj 2022. // www.kalix.se/Aktuellt/politik/kalix-hantering-av-it-attacken-gav-eko-i-hela-varlden/.

Kalix Kommun. Rapport IT-attacken socialförvaltningen Kalix kommun. No. 20220815. 2022.

Karlzen, Henrik, och Teodor Sommestad. *När luras personer av nätfiske? En genomgång av publicerade fältexperiment*. text FOI-R--4951--SE. FOI, 2020. https://intranet.foi.se/ovrigt/rapportsammanfattning.html?reportNo=FOI-R--4951--SE.

Mathur, Lakshya, Chole Vallabh, och Karnik Abhishek. ”The Scam Strikes Back: Exploiting the CrowdStrike Outage”. McAfee Blog, 30 juli 2024. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-scam-strikes-back-exploiting-the-crowdstrike-outage/.

Monsees, L. ”Information disorder, fake news and the future of democracy”. GLOBALIZATIONS 20, nr 1 (2023): 153–68. WOS:000654765300001. https://doi.org/10.1080/14747731.2021.1927470.

MSB. Cyberangrepp mot samhällsviktiga informationssystem 25 rekommendationer för stärkt skydd mot cyberangrepp. No. MSB2287. MSB, 2024. https://rib.msb.se/filer/pdf/30558.pdf.

NCSC UK. ”Log4j Vulnerability - What Everyone Needs to Know”. Log4j Vulnerability - What Everyone Needs to Know. Åtkomstdatum 08 oktober 2025. https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know.

Nilsson, Per-Erik, Sofia Olsson, och Ivar Ekman. Den nya informationsmiljöns topografi - Teknik, människa och strategi i osäkerhetens tidevarv. FOI-R--5342--SE. FOI Totalförsvarets Forskningsinstitut, 2022. https://www.foi.se/rest-api/report/FOI-R--5342--SE.

Nyheter, S. V. T. ”Detta vet vi: Kabelbrotten i Östersjön”. SVT Nyheter, 27 januari 2025. https://www.svt.se/nyheter/inrikes/detta-vet-vi-kabelbrotten-i-ostersjon.

Nyheter, S. V. T. ”Falska sms sprids – påstås att Sverige utsätts för väpnat angrepp”. SVT Nyheter, 05 september 2025. https://www.svt.se/nyheter/inrikes/falska-sms-sprids-pastas-att-sverige-utsatts-for-vapnat-angrepp.

Nyheter, S. V. T. ”Filmer visar drönarna över svenska kärnkraftverk”. SVT Nyheter, 14 april 2022. https://www.svt.se/nyheter/inrikes/filmer-visar-dronare-over-svenska-karnkraftverk.

Pamment, James, och Elsa Isaksson. Psychological Defence: Concepts and principles for the 2020s. MPF Report Series 6/2024. Myndigheten för psykologiskt försvar (MPF), 2024.

Pearson, James. ”Russia Downed Satellite Internet in Ukraine -Western Officials”. Europe. Reuters, 11 maj 2022. https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/.

Porada, Viktor, och Anton Lisník. ”Propaganda, Disinformation, Informational, Psychological and Mental Warfare as Instruments of Power in Globalized World”. Košická Bezpečnostná Revue 13, nr 2 (2023): 138–56.

SOS Alarm. ”Information med anledning av falska sms - SOS Alarm”. 05 september 2025. https://www.sosalarm.se/om-oss/pressrum/pressmeddelanden/2025/information-med-anledning-av-falska-sms/.

SÄPO. ”Förundersökning tas över kring drönare vid kärnkraftverk”. Text. 2022. http://sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2022-01-19-forundersokning-tas-over-kring-dronare-vid-karnkraftverk.html.

Viasat. ”KA-SAT Network Cyber Attack Overview”. Viasat.Com. Åtkomstdatum 08 oktober 2025. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/.

Wickström, Astrid, och Sara Schwartz Wiman. ”Grundproblemet löst efter globala it-störningar”. SVT Nyheter, 19 juli 2024. https://www.svt.se/nyheter/utrikes/it-storningar-varlden-over.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Tel: +46 8 5550 3000
www.foi.se