



UPPDATERAD SEPTEMBER 2025

RÖD MOT BLÅ

EN WORKSHOP FÖR ATT ÖKA MOTSTÅNSKRAFTEN MOT
OTILLBÖRLIG INFORMATIONSPÅVERKAN



INTRODUKTION

Det finns främmande makt och andra utländska hotaktörer som använder desinformation, vilseledning och propaganda för att skada Sverige. Alla delar av samhället påverkas när främmande makt använder otillbörlig informationspåverkan för att skada förtroendet, splittra och polarisera grupper för att skapa ett mer sårbart samhälle. Syftet med att sprida informationen är att påverka vad en befolkning tror, hur de beter sig och vilka beslut de fattar. Det skapar instabilitet i samhället och kan minska förtroendet för demokratin och samhällets funktioner. Denna workshop kan genomföras av aktörer som vill stärka sin förmåga att hantera otillbörlig informationspåverkan.

Workshopen har hämtat inspiration från rapporten: Sörensen, S. (2024) Enhancing Organizational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops. Riga: NATO Strategic Communications Centre of Excellence.¹

¹ stratcomcoe.org/publications/enhancing-organisational-capability-a-tailored-approach-with-red-team-vs-blue-team-adapted-workshops/299

FÖRBEREDELSE OCH PLANERING

Den här instruktionen riktar sig till er som ska vara moderatorer för Röd mot Blå. Materialet är utvecklat för två moderatorer samt en tydlig uppdragsgivare, som i sin tur ansvarar för att förvalta resultaten från utvärderingarna. Resultaten kan också förvaltas av moderatorerna på uppdrag av uppdragsgivaren.

I workshopen delas deltagarna in i två lag; röd och blå. Det röda laget använder påverkanstekniker mot det blå lagets organisation som i sin tur genomför motåtgärder mot det röda lagets aktiviteter.

MÅL OCH SYFTE

Röd mot Blå är utvecklad i syfte att öka förståelsen för hur otillbörlig informationspåverkan kan påverka den egna organisationen samt identifiera sårbarheter och ta fram underlag att arbeta vidare med.

MÅL :

- Ge exempel på hur påverkanstekniker kan användas inom otillbörlig informationspåverkan
- Välja lämpliga motåtgärder för att bemöta otillbörlig informationspåverkan

Materialet är anpassningsbart, mål och syfte anpassas utifrån era behov.

ANALYS OCH UTVÄRDERING

Presentera utvärderingsfrågorna i början av workshopen. Vi föreslår utvärdering på individnivå och organisatorisk nivå. Den går att genomföra på enklaste sätt, antingen muntligt eller skriftligt på post-it lappar.

- Vad tar du med dig från workshopen?
- Vad tycker du din organisation ska utveckla när det gäller att välja lämpliga motåtgärder för att bemöta otillbörlig informationspåverkan?

Moderatorerna sammanställer utvärderingen och lämnar över till uppdragsgivaren.

ENGAGERANDE FRÅGOR

Moderatorerna kan använda nedanstående frågor under workshopen eller i utvärderingen för att skapa ytterligare engagemang och lärande.

- Vilka funktioner och förmågor har ni för att upptäcka och hantera typhändelsen?

- När tror ni att er organisation behöver agera i typhändelsen?
- Vilka skulle ni samverka med internt och externt för att hantera typhändelsen?

TYPHÄNDELSE

En typhändelse beskriver startläge och händelseförlopp initierat av det röda laget. Välj en typhändelse som bedöms mest värdefull för organisationen. Typhändelserna finns beskrivna sist i detta dokument och delas med deltagarna vid workshopens start.

TIDSÅTGÅNG

Uppskattad tid för genomförande är en halvdag; en halvtimme för uppstart, en och en halv timme workshop, en timme utvärdering och diskussion (exklusive rast).

DELTAGARE

Workshopen är skapad för deltagare som kommer från samma organisation. De kan ha samma befattningar eller olika. Vi rekommenderar att deltagarantalet begränsas till fyra i respektive lag.

FÖRKUNSKAPER OCH STÖDJANDE DOKUMENT

Deltagarna bör ha kännedom om sårbarheter, påverkanstekniker och motåtgärder. Samtliga beskrivs i vår handbok "Att möta informationspåverkan – handbok för kommunikatörer". Den och ytterligare fördjupningar finns på Förmågeportalen på mpf.se. Varje lag bör ha minst ett exemplar av handboken samt egna relevanta planer och rutiner t ex kommunikation eller krishantering.

LAG BLÅ

Lag blå representerar sidan som försöker förhindra eller motverka otillbörlig informationspåverkan från det röda laget genom att välja motåtgärder.

LAG RÖD

Lag röd representerar en antagonistisk aktör som utnyttjar sårbarheter för att rikta en kampanj med påverkanstekniker mot lag blå.

LOKALER

Det behövs en lokal till två lag. Vissa lokaler kan vara lämpliga för fyra lag och två parallella workshops. Fler lokaler kan behövas.

SÄKERHETSSKYDD

Under workshopen behöver informationssäkerheten beaktas. Om exempelvis säkerhetsskyddsklassificerade eller sekretessbelagda uppgifter delas kan det ställa krav på deltagarnas behörighet att ta del av uppgifterna, samt lokalernas utformning.

FASINDELNING

Workshopen är indelad i ett antal faser där lagen tänker ut vilka påverkanstekniker respektive motåtgärder som de ska använda. Grundplaneringen är för sex faser, typhändelsen (fas 0), tre blå (fas 1,3 och 5) och två röda (fas 2 och 5) som varvas.

MODERATORER

Det bör finnas en moderator för två lag. Detta gör att workshopen kan skalas upp med fler lag och fler moderatorer.

MODERATORERNA :

- bokar lämplig lokal och möblerar i öar utifrån hur många lag som bjuds in
- tar med handböcker
- ser till att lagen kan visualisera åtgärder genom post-it lappar, White board eller Magic Wallpaper
- påminner deltagarna om att ta med planer och rutiner
- underlättar diskussioner genom förtydliganden
- uppmuntrar deltagande genom att verka för att alla kommer till tals och bidrar med sina insikter och idéer
- ansvarar för att anpassa tiden under workshopens faser
- leder utvärderingen

ANPASSNINGAR

I olika situationer kan det uppkomma behov av att justera ordinarie upplägg. Det kan exempelvis röra workshopens långsiktiga syfte, organisationsförändringar, tidsaspekter eller förkunskaper hos målgruppen. Här följer förslag på anpassningar för att justera workshopens genomförande:

- Deltagarnas tid under respektive fas begränsas ytterligare.
- Justering av antal medverkande deltagare i respektive lag – simulerar att resurser tillförs eller begränsas.
- Låt en av moderatorerna kommunicera lagens åtgärder. Alternativt kan lagen placeras i olika rum för att ytterligare försvåra för lagen att förstå varandras bakomliggande motiv.
- På förhand utpekade roller för deltagarna i respektive grupp/lag.
- Moderatoren kan löpande ge lagen olika förutsättningar. Exempelvis kan röd få ingångsvärdet att enbart använda sig av sociala medier.

GENOMFÖRANDE

WORKSHOPMETOD OCH STRUKTUR

Fas 0: Moderatoren presenterar den typhändelse som valts. Typhändelsen ska visualiseras så enkelt som möjligt, exempelvis projicerad bild, White board eller utdelad på papper. Typhändelsen fungerar som startläget för det blå laget för vad det röda laget redan gjort. Moderatoren meddelar hur lång tid lagen får i respektive fas, vilken kan anpassas efterhand för att förenkla eller försvåra. Lagen får lyssna på varandra när de diskuterar eftersom de är i samma lokal.

Fas 1: Det blå laget diskuterar sårbarheter samt vilka resurser, planer och rutiner de har för att genomföra motåtgärder baserade på de tekniker som beskrivs. Beslutade åtgärder visualiseras och presenteras för moderatorerna och det röda laget.

Fas 2: Det röda laget diskuterar vilka sårbarheter de ska nyttja och beslutar om vilka påverkanstekniker de vill använda mot det blå laget. Beslutade tekniker sätts in i en kontext, visualiseras och presenteras för moderatorerna och det blå laget.

Fas 3: Det blå laget diskuterar igen sårbarheter samt vilka resurser, planer och rutiner de har för att genomföra motåtgärder baserade på de tekniker som det röda laget använder. Beslutade åtgärder visualiseras och presenteras för moderatorerna och det röda laget.

Fas 4: Det röda laget diskuterar åter vilka sårbarheter de ska nyttja och beslutar om vilka påverkans-tekniker de vill använda mot det blå laget. Beslutade tekniker sätts in i en kontext, visualiseras och presenteras för moderatorerna och det blå laget.

Fas 5: Det blå laget diskuterar på nytt sårbarheter samt vilka resurser, planer och rutiner de har för att genomföra motåtgärder baserade på de tekniker som det röda laget använder. Beslutade åtgärder visualiseras och presenteras för moderatorerna och det röda laget.

AVRUNDNING:

När målen med workshopen är uppfyllda kan moderatorerna säga att det röda lagets resurser blir prioriterade till andra uppgifter och workshopen kan rundas av. Moderatorerna kan också styra workshopen så att det blir fler faser om det finns tid.

ANALYS OCH UTVÄRDERING:

Moderatorerna återknyter till målen med workshopen och genomför en utvärdering. Presentera utvärderingsfrågorna för deltagarna på enklaste sätt, antingen muntligt eller skriftligt på post-it lappar.

- Vad tar du med dig från workshopen?
- Vad tycker du din organisation ska utveckla när det gäller att välja lämpliga motåtgärder för att bemöta otillbörlig informationspåverkan?

Låt deltagarna först tänka igenom och skriva ned svaren enskilt under någon minut. Därefter diskutera sina svar med en annan deltagare i några minuter och slutligen dela sina insikter i en större grupp (om fyra deltagare eller med alla).

Moderatorerna samlar in och sammanställer de skriftliga utvärderingarna och lämnar över dessa till uppdragsgivaren. Utvärderingarna kan bidra till fortsatt verksamhetsutveckling och ökad motståndskraft.

De engagerande frågorna går att använda sig av i en avslutande diskussion.

FAS 0	FAS 1	FAS 2	FAS 3	FAS 4	FAS 5
TYP-HÄNDELSE	BLÅ	RÖD	BLÅ	RÖD	BLÅ

TYPHÄNDELSE

1. DEMONSTRATIONER

Under det gångna året har människor blivit frustrerade över inflationen och de ökade kostnaderna för mat, bränsle och energi. Detta har föranlett en hårdare retorik kring situationen på sociala medier och i internationella nyhetsmedier. Både utländsk statskontrollerad media och fristående media delar artiklar med hård retorik om landets situation. En sluten grupp på en social medieplattform har planerat en demonstration utanför din arbetsplats, som ses som representativ för den offentliga sektorn. En stor folksamling samlas och ropar att du är ansvarig för den situation som samhället befinner sig i. Det finns en oro för att detta kan bli mer våldsamt.

Narrativ: Staten har misslyckats eftersom den inte kan lindra krisen. Om du inte stöder regeringen finns det ingen yttrandefrihet. Regeringens utrikespolitik är skadlig för landet.

Tekniker: Falsk information sprids i slutna sociala mediegrupper. Webbplatser, bloggar och YouTube-kanaler som fungerar som alternativa mediekkanaler sprider desinformation med hjälp av 'experter'. Även korrekt information sprids men användes i skadliga sammanhang.

OFFENTLIGA DEMONSTRATIONER

Legitima demonstrationer är symboliska handlingar som används för att främja ett visst politiskt ämne eller position. De är en viktig del av den demokratiska dialogen. Fientliga aktörer kan dock orkestrera demonstrationer för att felaktigt ge intryck av starkt stöd eller ogillande av en viss fråga.

EKOKAMMARE

Undergrupper där människor kommunicerar främst med andra som har liknande åsikter och övertygelser kallas ekokammare; de existerar både online och i verkliga livet. Till exempel är personer med liknande åsikter troliga att läsa samma tidningar och umgås med varandra och kan därför sällan bli exponerade för ideologiskt olika åsikter. Detta kan utnyttjas online för att sprida riktad information till specifika grupper.

BOTAR

Botar är datorprogram som utför automatiserade uppgifter, till exempel att dela vissa typer av information på sociala medier eller för att svara på vanliga frågor på en kundtjänstplattform. Inom informationspåverkan kan de användas till att förstärka utvalda budskap på nätet, spamma forum och kommentarsfält, gilla eller dela inlägg på sociala medier, eller för att genomföra cyberattacker.

BANDWAGON EFFEKT

Människor som känner att de tillhör majoriteten är mer benägna att uttrycka sina åsikter. Botar kan öka antalet gilla-markeringar, kommentarer och delningar på ett inlägg på sociala medier för att ge intryck av social acceptans. Detta tilltalar det kognitiva behovet av tillhörighet och underlättar ytterligare engagemang från faktiska mänskliga användare.

2. CYBERINCIDENT

Frekventa cyberattacker har drabbat olika delar av samhället de senaste månaderna. Även er organisation har blivit utsatt där ett intrång har lett till att era gemensamma lagringsytor drabbats. Informationen där har flyttats om och nyligen laddats upp på nytt. Såvitt ni kan bedöma saknas flera filer och dokument, och nya har lagts till. Er organisation har ännu inte hunnit få en helhetsbild över vad som skett med alla dokument. Samtidigt publiceras nyheter om att dokument läckts och sägs påvisa att er högsta beslutsfattare förskingrat organisationens pengar.

Narrativ: Alla nivåer i samhället är korrupta. Man kan inte lita på offentliga aktörer.

Tekniker: Genom att hacka ert nätverk har någon gjort det rimligt att ifrågasätta säkerheten i era system och om ni är komprometterade. Detta undergräver förtroendet för det specifika systemet eller den ansvariga verksamheten. Att läcka stulen information har stort symboliskt värde eftersom detta tidigare genomförts för att påvisa orättvisor och nedtystade fakta som inte var känt för allmänheten.

NÄTFISKE

Nätfiske är en teknik som lurar användare att uppges lösenord eller annan känslig information på internet. Nätfiske omfattar även automatiserad spamning via e-postmeddelanden som framstår som om de skickats från en känd avsändare men som egentligen tillhör en bedragare som är ute efter personlig information. Spjutfiske (spear-phishing) är en sofistikerad typ av nätfiske för att komma åt information på säkra datorsystem.

HACKNING

Hackning innebär att skaffa sig obehörig åtkomst till en dator eller ett nätverk, och är i sig ett brott. Inom informationspåverkan fungerar hackning ibland som en symbolisk handling där själva intrånget är sekundärt. Det egentliga målet är att väcka misstanke om att ett system är exponerat eller osäkert, vilket kan underminera förtroendet för systemet ifråga eller en organisation med ansvar för detsamma.

FÖRFALSKNINGAR

Att fabricera och förfalska information är ett effektivt sätt att få desinformation att framstå som autentisk information. Falsa sidhuvuden, stämplat eller namnteckningar kan användas för att få rena falskarier att se äkta ut.

LÄCKOR

Läckor har en stark symbolisk betydelse eftersom de kan avslöja orättvisor och mörkläggnings som annars inte kommit till allmänhetens kännedom. Inom informationspåverkan tas dock läckt information ofta ur sitt sammanhang och används för att systematiskt undergräva en aktörs trovärdighet och förvränga informationsmiljön. Den läckta informationen kan ha erhållits exempelvis genom datorintrång eller stöld.

TYPHÄNDELSER

3. ÖKADE HYBRIDHOT OCH SOCIAL ORO

Nato har skickat trupper till den ukrainska gränsen och de senaste månaderna har cyberattacker och kränkningar av svenskt luftrum skett upprepade gånger. På många platser i samhället sker diskussioner kring om detta kan vara de första tecknen på en stundande invasion av Sverige. Statliga myndigheter fastslår att de inte ser det som troligt inom den närmsta framtiden. Det sprids desinformation om riskerna med vårt Natomedlemskap som ifrågasätts i vissa grupper. Dessa diskussioner sker främst på sociala medier och i slutna grupper. Det pågående beredskapsarbete som sker i samhället orsakar indirekta effekter såsom oro och förvirring hos allmänheten kring vad som egentligen händer och vem som är ansvarig.

Narrativ: Nato är ett hot mot Sveriges nationella intressen. Sveriges försvarsmakt är underdimensionerad och/eller inkompetent. Nato kommer inte hjälpa Sverige. Personer som är krigsplacerade i en stridande roll kommer vara kanonmat.

Tekniker: Sociala medier och botar används för att sprida idéer och argument som ger en snedvriden bild av landet och dess Natomedlemskap. Särskilt TikTok, Instagram och marginaliserade medier (webbplatser, bloggar, YouTube-kanaler) sprider en stor mängd förvrängda budskap.

FALSKT ELLER FELAKTIGT SAMMANHANG

Presentation av korrekt fakta i ett orelaterat sammanhang för att framställa en fråga, händelse eller person på ett vilseledande sätt. Till exempel kan bilder tagna i andra sammanhang användas för att förstärka narrativet i en nyhetsartikel.

KAPNING AV ARGUMENT OCH HALMGUBBAR

Ett exempel på kapning är att ta över en pågående debatt och ändra dess syfte eller ämne. Detta är särskilt effektivt när det tillämpas på hashtags och memes, och kan även användas för att störa evenemang eller motkulturella sociala rörelser.

Ett halmgubbe-argument används för att diskreditera en motståndare genom att tillskriva dem argument eller ståndpunkter som de inte håller med om, och sedan argumentera mot dessa ståndpunkter.

BOTAR

Botar är datorprogram som utför automatiserade uppgifter, till exempel att dela vissa typer av information på sociala medier eller för att svara på vanliga frågor på en kundtjänstplattform. Inom informationspåverkan kan de användas till att förstärka utvalda budskap på nätet, spamma forum och kommentarsfält, gilla eller dela inlägg på sociala medier, eller för att genomföra cyberattacker.

FALSKA MEDIER

Desinformation kan spridas genom att skapa falska medieplattformar som ser ut som, eller har en webbadress liknande, en riktig nyhetssida. Det är relativt enkelt och billigt att skapa en falsk webbplats online som ser nästan identisk ut med en riktig webbplats men publicerar helt annat innehåll.

4. RADIOAKTIV LÄCKA

Det har skett en explosion vid ett kärnkraftverk i Ukraina, vilket har lett till radioaktiv förorening av det omgivande området. Experter säger att radioaktiva partiklar kan förväntas sprida sig till norra Europa på grund av vindriktningen. Jämfört med Tjernobykatas trofen kommer dock sannolikt endast små radioaktiva partiklar att detekteras, som inte bedöms påverka människor på lång sikt. Trots experternas bedömning börjar människor att få panik och spekulera. Individer som påstår sig vara experter intervjuas i alternativa medier (främst på YouTube-kanaler) och säger att konsekvenserna kommer att vara förödande för Sverige, och att vi inte kan vara säkra på att politikerna kommer berätta hela sanningen för att undvika panik. Viss traditionell media publicerar av misstag några av dessa falska påståenden. En effekt blir att människor hamstrar jodtabletter och skyddsutrustning, vilket gör det svårare för aktörer som använder detta i sitt arbete att få leveranser när det verkligen krävs.

Narrativ: Alla kommer påverkas. Du kan skydda dig. Du är säker om du följer dessa steg (irrationella skyddsåtgärder). Politiker ljugar för oss.

Tekniker: Falska experter används och sänds på sociala medieplattformar. Sanningen blandas med desinformation. Det är svårt att förklara för befolkningen vad som är sant och vad som inte är sant angående de förväntade effekterna av strålningen. Falska bilder från platsen sprids och visar en mycket större explosion och större skador än vad som faktiskt är fallet.

IMITATÖRER OCH BEDRAGARE

Imitatorer låtsas att de är någon annan än de egentligen är, dvs. ikläder sig någon annans identitet. Det kan röra sig om bedragare som påstår sig ha expertkunskap eller kvalifikationer de egentligen saknar, som att utge sig för att vara läkare eller advokat utan att ha genomgått den utbildning som krävs.

POTEMKINKULISSER

Resursstarka aktörer kan gå ett steg längre och skapa falska och vilseledande institutioner och nätverk. Falska företag, forskningsinstitut och tankesmedjor är exempel på det som kallas potemkinkulisser som kan skapas och användas för att skänka äkthet till desinformation.

FALSKT ELLER FELAKTIGT SAMMANHANG

Presentation av korrekt fakta i ett orelaterat sammanhang för att framställa en fråga, händelse eller person på ett vilseledande sätt. Till exempel kan bilder tagna i andra sammanhang användas för att förstärka narrativet i en nyhetsartikel.

TYPHÄNDELSE

5. AI OCH DEEPPFAKE

En video på statsministern blir viral på sociala medieplattformar (främst på TikTok och Instagram). I videon ses statsministern hålla en presskonferens där er organisation påstås vara en del i ett korrupsionsnätverk. Regeringen är snabb med att gå ut med en dementi och informerar om att videon är en sofistikerad förfälskning. Trots detta följer hatkommentarer och er organisation mottar hot och en av era lokaler utsätts för vandalism.

Narrativ: Offentliga aktörer är korrupta och går inte att lita på. Den här specifika organisationen förskingrar skattemedel.

Tekniker: en avancerad deepfake cirkulerar på sociala medier och algoritmer påverkas av botar som ökar visningar, likes och delningar.

DEEPPFAKES

Moderna inlärningsalgoritmer kan användas för att manipulera ljud och video på väldigt avancerade sätt. Man kan exempelvis producera falska men väldigt trovärdiga videoklipp där politiker läser upp påhittade tal. Man kan även byta ansikten på personer i befintliga videoklipp eller rekonstruera en persons röst digitalt.

BOTAR

Botar är datorprogram som utför automatiserade uppgifter, till exempel att dela vissa typer av information på sociala medier eller för att svara på vanliga frågor på en kundtjänstplattform. Inom informationspåverkan kan de användas till att förstärka utvalda budskap på nätet, spamma forum och kommentarsfält, gilla eller dela inlägg på sociala medier, eller för att genomföra cyberattacker.





**Myndigheten för
psykologiskt försvar**



MYNDIGHETEN FÖR PSYKOLOGISKT FÖRSVAR
VÅXNÄSGATAN 10
653 40 KARLSTAD
REGISTRATOR@MPF.SE
010 - 183 70 00
WWW.MPF.SE