Psychological Defence Agency

UPDATED SEPTEMBER 2025

RED AGAINST BLUE

A WORKSHOP FOR INCREASING RESILIENCE TO MALIGN INFORMATION INFLUENCE

INTRODUCTION

Antagonistic foreign powers and other foreign threat actors can use disinformation, misleading information and propaganda to harm Sweden. All parts of society are affected when foreign powers use malign information influence to damage trust, divide and polarise groups to create a more vulnerable society. The purpose of disseminating the information is to sway a population's beliefs, behaviour and decisions. It creates instability in society and can undermine confidence in democracy and society's functions. This workshop can be held by actors wishing to strengthen their capabilities for dealing with malign information influence.

The workshop was inspired by the report: 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

PREPARATIONS AND PLANNING

These instructions are intended for Red against Blue moderators. The materials have been developed for two moderators and a clear principal which, in turn, is responsible for handling the results from the evaluations. The results can also be handled by the moderators on behalf of the principal.

In the workshop, participants are divided into two teams – red and blue. The red team uses influence tactics against the blue team's organisation, which in turn implements countermeasures against the red team's activities.

OBJECTIVE AND PURPOSE

Red against Blue has been developed to improve understanding of how malign information influence can affect your own organisation, and identify vulnerabilities and produce materials for continuing efforts.

GOALS:

- Provide examples of how influence tactics can be used in malign information influence
- Choose appropriate countermeasures to tackle malign information influence

The material is adaptable – objective and purpose are adapted to your needs.

ANALYSIS AND EVALUATION

Present the evaluation questions at the beginning of the workshop. We suggest evaluation at the individual level and organisational level. This can be done in the simplest way, either verbally or in writing on post-it notes.

- What do you take with you from the workshop?
- What do you think your organisation should develop in terms of choosing appropriate countermeasures to tackle malign information influence?

The moderators compile the evaluation and submit it to the principal.

ENGAGING QUESTIONS

The moderators can use the following questions during the workshop or in the evaluation to create further engagement and learning.

- What functions and capabilities do you possess for detecting and managing the typical incident?
- When do you think your organisation needs to act in the typical incident?
- Who would you work with internally and externally to manage the typical incident?

TYPICAL INCIDENT

A typical incident describes the starting point and sequence of events initiated by the red team. Choose a typical incident that is considered most valuable for your organisation. The typical incidents are described at the end of this document and are shared with participants at the beginning of the workshop.

TIME REQUIRED

The estimated time for holding the workshop is half a day – half an hour for start-up, workshop of an hour and a half, one hour evaluation and discussion (excluding break).

PARTICIPANTS

The workshop is designed for participants who come from the same organisation. They may hold the same or different positions. We recommend limiting the number of participants to four in each team.

PRIOR KNOWLEDGE AND SUPPORTING DOCUMENTS

Participants should be familiar with vulnerabilities, influence tactics and countermeasures. All of these are described in our handbook "Countering

malign information influence – Handbook for communicators". That and more in-depth information are available in the Capabilities Portal at mpf.se. Each team should have at least one copy of the handbook and its own relevant plans and procedures, such as for communication or crisis management.

TEAM BLUE
Team blue represents the side that is attempting to prevent or counteract malign information influence from the red team by choosing countermeasures.

TEAM RED
Team red represents an antagonistic actor that exploits vulnerabilities to wage a campaign of influence tactics against team blue.

VENUE
One venue for two teams is needed. Some venues may be suitable for four teams and two parallel workshops. More venues may be needed.

PROTECTIVE SECURITY
During the workshop, account needs to be taken of information security. For example, sharing information classified under protective security or confidential information may place demands in terms of participants' permission to access the information, and venue layout.

BREAKDOWN INTO STAGES
The workshop is divided into a number of stages in which the teams devise the influence tactics and countermeasures they will use. The basic planning is for six stages – the typical incident (stage 0), three blue (stage 1, 3 and 5) and two red (stage 2 and 5), which are alternated.

MODERATORS
There should be one moderator for two teams. This enables the workshop to be scaled up with more teams and more moderators.

THE MODERATORS:
- book an appropriate venue and arrange furniture in islands based on the number of teams invited
- bring handbooks
- ensure that the teams can visualise measures through post-it notes, a whiteboard or Magic Wallpaper
- remind participants to bring plans and procedures
- facilitate discussions through clarifications
- encourage participation by seeking to ensure that everybody has their voice heard and contributes their insights and ideas
- are responsible for adapting the time spent on the workshop stages
- lead the evaluation

ADAPTATIONS
In different situations, there may be a need to adjust the regular structure. This may include, for example, the long-term purpose of the workshop, organisational changes, time aspects or the target group's prior knowledge. The following are suggestions for adapting the workshop:

- Further limiting the participants' time during each stage.
- Adjusting the number of participants in each team (simulating adding or cutting resources).
- Letting one of the moderators communicate the teams' measures. Alternatively, the teams can be placed in different rooms to make it more difficult for them to understand each other's underlying motives.
- Designating roles in advance for the participants in each group/team.
- The moderator can continuously set different conditions for the teams. For example, red can be told at the outset that it can only use social media.

WORKSHOP PROCESS

WORKSHOP METHOD AND STRUCTURE

Stage 0: The moderator presents the selected typical incident. The typical incident should be visualised as simply as possible – for example as an image on a projector, whiteboard or on a paper handout. The typical incident serves as the starting point for the blue team for what the red team has already done. The moderator communicates how much time the teams will have in each stage, which can be subsequently adapted to make things easier or more difficult. The teams may listen to each other when discussing as they are in the same venue.

Stage 1: The blue team discusses vulnerabilities as well as the resources, plans and procedures it has in place for implementing countermeasures based on the described tactics. Decided measures are visualised and presented to the moderators and the red team.

Stage 2: The red team discusses the vulnerabilities it will exploit and decides on the influence tactics it wishes to use against the blue team. Decided tactics are put into a context, visualised and presented to the moderators and the blue team.

Stage 3: The blue team discusses again vulnerabilities as well as the resources, plans and procedures it has in place for implementing countermeasures based on the tactics used by the red team. Decided measures are visualised and presented to the moderators and the red team.

Stage 4: The red team discusses again the vulnerabilities it will exploit and decides on the influence tactics it wishes to use against the blue team. Decided tactics are put into a context, visualised and presented to the moderators and the blue team.

Stage 5: The blue team discusses once more vulnerabilities as well as the resources, plans and procedures it has in place for implementing countermeasures based on the tactics used by the red team. Decided measures are visualised and presented to the moderators and the red team.

ROUNDING OFF THE WORKSHOP:

Once the goals of the workshop have been attained, the moderators can say that the red team's resources will be prioritised for other tasks and the workshop can be rounded off. The moderators can also steer the workshop so that there are more stages, time permitting.

ANALYSIS AND EVALUATION:

The moderators refer back to the workshop objectives and perform an evaluation. Present the evaluation questions to participants in the simplest way, either verbally or in writing on post-it notes.

- What do you take with you from the workshop?
- What do you think your organisation should develop in terms of choosing appropriate countermeasures to address malign information influence?

First, let the participants consider and write down the answers individually for a few minutes. Then, they discuss their answers with another participant for a few minutes and finally they share their insights in a larger group (of four participants or with everyone).

The moderators collect and compile the written evaluations and hand them over to the principal. The evaluations can contribute to continuing operational development and heightened resilience.

The engaging questions can be used in a final discussion.

STAGE 0	STAGE 1	STAGE 2	STAGE 3	STAGE 4	STAGE 5
TYPICAL INCIDENT	BLUE	RED	BLUE	RED	BLUE

TYPICAL INCIDENTS

1. DEMONSTRATIONS

Over the past year, people have become frustrated with inflation and the rising costs of food, fuel and energy. This has led to harsher rhetoric concerning the situation on social media and in international news media. Both foreign state-controlled media and independent media share articles with harsh rhetoric about the country's situation. A closed group on a social media platform has planned a demonstration outside your workplace, which is seen as representative of the public sector. A large crowd gathers and cries out that you are responsible for the current state of society. There are fears that the situation could turn more violent.

Narrative: The state has failed because it cannot ease the crisis. If you do not support the government, there is no freedom of speech. The government's foreign policy is harmful for the country.

Tactics: False information is spread in closed social media groups. Websites, blogs and YouTube channels that serve as alternative media channels spread disinformation with the help of "experts". Accurate information is also disseminated but used in harmful contexts.

PUBLIC DEMONSTRATIONS
Legitimate demonstrations are symbolic actions that are used to promote a particular political topic or position. They are an important part of democratic dialogue. Hostile actors, however, may orchestrate demonstrations to give a false impression of strong support or disapproval of a particular issue.

ECHO CHAMBER
Subgroups in which people communicate mainly with others who hold similar views and beliefs are called echo chambers – they exist both online and in real life. For example, people with similar opinions are likely to read the same newspapers and socialise with each other and can therefore rarely be exposed to ideologically different opinions. Online, this can be exploited to spread targeted information to specific groups.

BOTS
Bots are computer programs that perform automated tasks, such as sharing certain types of information on social media or answering frequently asked questions on a customer services platform. In information influence, they can be used to reinforce selected messages online, spam forums and comment sections, like or share posts on social media, or to perpetrate cyberattacks.

BANDWAGON EFFECT
People who feel they belong to the majority are more likely to express their opinions. Bots can increase the number of likes, comments, and shares for a post on social media to give the impression of social acceptance. This appeals to the cognitive need for belonging and facilitates further engagement from actual human users.

TYPICAL INCIDENTS

2. CYBER INCIDENT

Frequent cyberattacks have struck various parts of society in recent months. Your organisation has also been subjected, with a data intrusion affecting your common storage areas. The data stored there has been moved and recently uploaded again. As far as you can judge, numerous files and documents are missing, and new ones have been added.
Your organisation has not yet been able to gain a comprehensive grasp of what has happened to all the documents. At the same time, news stories are published about documents having been leaked, claiming to show that your top decision-maker has embezzled the organisation's money.

Narrative: All levels of society are corrupt. Public-sector actors cannot be trusted.

Tactics: By hacking into your network, someone has made it reasonable to question the security of your systems and whether you are compromised. This undermines trust in the specific system or the responsible operations. Leaking stolen information has tremendous symbolic value as this has been done in the past to uncover injustices and hushed facts that were not publicly known.

PHISHING
Phishing is a technique that tricks users into entering passwords or other sensitive information online. Phishing also includes automated spamming through e-mails that appear to have been sent from a known sender, but that actually belong to a scammer in search of personal information. Spear-phishing is a sophisticated type of phishing to access information in secure data systems.

HACKING
Hacking involves gaining unauthorised access to a computer or network, and is a crime in itself. In malign information influence, hacking sometimes works as a symbolic action in which the intrusion itself is secondary. The real objective is to raise suspicion that a system is exposed or insecure, which can undermine confidence in the system in question or an organisation responsible for it.

FORGERIES
Fabricating and falsifying information is an effective way to make disinformation look like authentic information. False page headers, stamps or signatures can be used to make outright forgeries look genuine.

LEAKS
Leaks have a strong symbolic significance as they can divulge injustices and cover-ups that would not otherwise have come to light. In malign information influence, however, leaked information is often taken out of context and used to systematically undermine an actor's credibility and distort the information landscape. The leaked information may have been obtained, for example, through data intrusion or theft.

TYPICAL INCIDENTS

3. HEIGHTENED HYBRID THREATS AND SOCIAL UNREST

NATO has sent troops to the Ukrainian border, and in recent months there have been repeated cyberattacks and violations of Swedish airspace. In many parts of society, there are discussions about whether this could be the first signs of an impending invasion of Sweden. Government officials establish that they do not see this as likely in the near future.

Disinformation is being spread about the risks of our NATO membership, which is being questioned in certain groups. These discussions are mainly found on social media and in closed groups. The ongoing contingency efforts under way in society cause indirect effects such as unease and confusion among the general public about what is actually going on and who is responsible.

Narrative: NATO is a threat to Sweden's national interests. The Swedish Armed Forces are underdimensioned and/or incompetent. NATO will not help Sweden. People with wartime postings in a combat role will be cannon fodder.

Tactics: Social media and bots are used to spread ideas and arguments that give a distorted picture of Sweden and its NATO membership. In particular, TikTok, Instagram and marginalised media (websites, blogs, YouTube channels) are spreading a high volume of distorted messages.

FAKE OR FALSE CONTEXT
Presentation of accurate facts in an unrelated context to portray an issue, event or person in a misleading way. For example, pictures taken in other contexts can be used to reinforce the narrative of a news article.

HIJACKING THE DEBATE AND STRAWMEN
An example of hijacking is to take over an ongoing debate and alter its purpose or topic. This is particularly effective when applied to hashtags and memes, and can also be used to disrupt events or countercultural social movements.

A strawman argument is used to discredit an opponent by assigning arguments or positions to them with which they disagree, and then arguing against those positions.

BOTS
Bots are computer programs that perform automated tasks, such as sharing certain types of information on social media or answering frequently asked questions on a customer services platform. In information influence, they can be used to reinforce selected messages online, spam forums and comment sections, like or share posts on social media, or to perpetrate cyberattacks.

FAKE MEDIA
Disinformation can be spread by creating fake media platforms that look like, or have a URL similar to, an authentic news site. It is relatively simple and inexpensive to create a fake website online that looks almost identical to an authentic website, but publishes completely different content.

TYPICAL INCIDENTS

4. RADIOACTIVE LEAK

There has been an explosion at a nuclear power plant in Ukraine, which has led to radioactive contamination of the surrounding area. Experts say that radioactive particles can be expected to spread to northern Europe due to wind direction. However, compared to the Chernobyl disaster, only minor radioactive particles will likely be detected, which are not judged to have any long-term effect on people. Despite the experts' assessment, people are starting to panic and speculate. Individuals claiming to be experts are interviewed in alternative media (mainly on YouTube channels) and say that the consequences will be devastating for Sweden, and that we cannot be sure that politicians will tell the whole truth to avoid panic. Some traditional media mistakenly publish some of these false claims. People stockpile iodine tablets and protective equipment, making it difficult for the actors involved, and purchasing them for needed work.

Narrative: Everyone will be affected. You can protect yourself. You will be safe if you follow these steps (irrational protection measures). Politicians are lying to us.

Tactics: Fake experts are used and broadcast on social media platforms. Truth is mixed with disinformation. It is difficult to explain to the population what is true and what is not about the expected effects of the radiation. Fake images from the site are spread, showing a much larger explosion and greater damage than in reality.

IMPERSONATORS AND FRAUDSTERS
Impersonators pretend that they are someone other than who they really are – that is, they assume someone else's identity. These can be fraudsters who claim to possess expertise or qualifications they actually lack, such as pretending to be a doctor or a lawyer without having obtained the necessary qualifications.

POTEMKIN VILLAGES
Resourceful actors can go one step further and create fake and misleading institutions and networks. Fake companies, research institutes and think tanks are examples of what are known as potemkim villages, which can be created and used to make disinformation look authentic.

FAKE OR FALSE CONTEXT
Presentation of accurate facts in an unrelated context to portray an issue, event or person in a misleading way. For example, pictures taken in other contexts can be used to reinforce the narrative of a news article.

TYPICAL INCIDENTS

5. AI AND DEEPFAKE

A video of the Prime Minister goes viral on social media platforms (mainly on TikTok and Instagram). In the video, the Prime Minister is holding a press conference at which your organisation is alleged to be part of a corruption network. The government is quick to issue a denial and communicate that the video is a sophisticated forgery. Nevertheless, hate comments follow and your organisation receives threats and one of your premises is vandalised.

Narrative: Public-sector actors are corrupt and cannot be trusted. This specific organisation is embezzling tax funds.

Tactics: An advanced deepfake is circulating on social media and algorithms are affected by bots that amplify views, likes and shares.

DEEPFAKES
Modern learning algorithms can be used to perform highly advanced manipulation of audio and video. For example, fake but highly credible video clips in which politicians read out fabricated speeches can be produced. People's faces can also be replaced in video clips, or their voices can be digitally modified.

BOTS
Bots are computer programs that perform automated tasks, such as sharing certain types of information on social media or answering frequently asked questions on a customer services platform. In malign information influence, they can be used to amplify selected messages online, to spam forums and comments sections, to like or share social media posts or to commit cyberattacks.

Psychological Defence Agency

PSYCHOLOGICAL DEFENCE AGENCY
VÄXNÄSGATAN 10
SE-653 40 KARLSTAD
REGISTRATOR@MPF.SE
+4610 183 70 00
WWW.MPF.SE