

**Psychological
Defence Agency**





PSYCHOLOGICAL DEFENCE AGENCY

We defend and safeguard our open and democratic society and the free formation of opinions.

Our mission

- Identify, analyze and provide support in countering malign information influence and other misleading information that is directed at Sweden or Swedish interests by antagonistic foreign powers.
- Build resilience against FIMI in agencies, municipalities, regions, companies and organizations, and the Swedish population.

Psychological defence

- Psychological defence is society's common capabilities for detecting and resisting malign information influence directed at Sweden by antagonistic foreign powers.
- The purpose of the psychological defence is to protect the open and democratic society, freedom of opinion and Sweden's freedom and independence.
- The ability to be a part of the democratic discussion and evaluate the validity of information is essential for psychological defence and our democracy.



Du är en del av Sveriges psykologiska försvar



Var uppmärksam på
falsk och vilseledande
information



Tänk efter innan
du delar information
på nätet



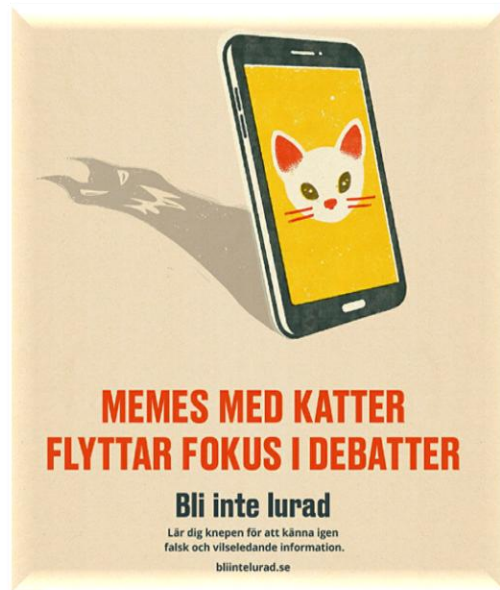
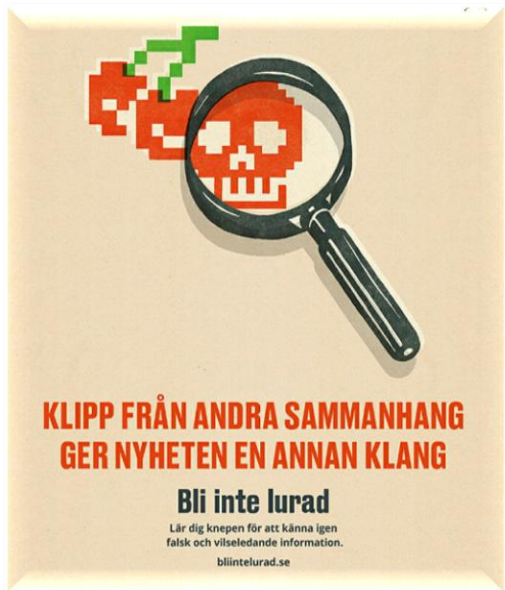
**Ta del av bekräftad
information** från
myndigheter

**Psychological
Defence Agency**



Information influence activities

- The use of information in a covert or deceptive manner to influence our opinions, perceptions, and decision-making to the benefit of someone else.
- Information influence is potentially harmful communication that is orchestrated by foreign powers or their agents.



Psychological
Defence Agency



Targeting vulnerabilities

Target audience

Strategic narratives

Information influence techniques



MALICIOUS RHETORIC

- Ad hominem
- Whataboutism
- Gish-gallop
- Strawman
- Hijacking



SOCIAL AND COGNITIVE HACKING

- Dark ads
- Bandwagon effects
- Spiral of silence
- Echo chambers and filter bubbles



DESINFORMATION

- Fabrication
- Manipulation
- Misappropriation
- Satire and parody



DECEPTIVE IDENTITIES

- Shills
- Impostors and cheats
- Counterfeits
- Potemkin villages
- Fake media



TECHNICAL EXPLOITATION

- Bots
- Sockpuppets
- Deepfakes
- Phishing



SYMBOLIC ACTIONS

- Leaking
- Hacking
- Public demonstrations

- Media system
- Public opinion formation
- Cognitive vulnerabilities



LEVEL 1: ASSESS

To understand what you are dealing with you must assess the situation. What is really going on? Who is involved? What is at stake? The more knowledge you have about the situation, the better your response will be.

MAP THE SITUATION

Analyse the situation and develop your awareness about what is happening. Use the tools discussed in Parts I & II to determine what you are dealing with.

FACT CHECK

Ascertain the facts of the situation — what is true/correct?

INVESTIGATE TRANSPARENTLY

Engage reliable independent actors, such as journalists, in investigating the issue and ensure transparency.



LEVEL 2: INFORM

Once you have made your assessment, you can start communicating with your target audiences. Focus on providing neutral information and facts, and let people know how you are dealing with the situation. Remember to adapt your messages for each audience/stakeholder group.

MAKE A STATEMENT

Lay out the facts of the case as you see them in a neutral manner.

CORRECT

Make a statement that directly responds to false allegations with relevant facts. Using and FAQ-style fact sheet can be a useful.

REFER

In cases where independent actors or sources can corroborate facts, it may be useful to refer to them as a source to strengthen your case.

ASSERT VALUES

Remind your audiences of what your organisation stands for.

NOTIFY STAKEHOLDERS

Be they colleagues or key stakeholders, the sooner you can let people know what is going on, the better.

ISSUE A HOLDING STATEMENT

Communicate that you are looking into the situation by issuing a holding statement. This will give you time to develop a more thorough response.

Fact-based response



LEVEL 3: ADVOCATE

Advocacy is one step up from providing neutral information and involves arguing your case more actively. Always consider your mandate and remind yourself of good communication practices and your organisation's values when designing your response.

DIALOGUE

Actively engage in a dialogue with key stakeholders and members of the public to involve them in responding to the issue.

FACILITATION

Make it easy for information to reach your key audiences. Organise events or meetings that bring different stakeholders together to discuss a specific problem and give you the opportunity to clarify your position.

MULTIPLIERS

Engage with key communicators who can help you spread your message to relevant audiences.

PIGGYBACKING

Use existing events, initiatives, or debates to promote the facts of the case.

FORMAL STATEMENT

Prepare a dossier that describes the course of events and presents facts that support your case. It is very important that this document is based on facts and verified information.

STORYTELLING

Relate the situation to a broader narrative about, for example, your organisation and its values, which will help your key audiences understand the situation and verify your position.



LEVEL 4: DEFEND

Defending involves designing a direct response to the aggressor. This step can appear controversial and should therefore be reserved for extreme cases. Be sure to discuss all actions at this level with colleagues and leadership first, to avoid exceeding your mandate or aggravating the situation.

IGNORE

Sometimes the best response is to do nothing. This might be suitable if information influence has been clearly determined but has not attracted much attention. In such cases an active response might further disseminate disinformation.

REPORT

If an attacker breaks the law or transgresses a social media platform's code of conduct, report them to the police or to the platform. This action should not be taken lightly or abused — use only in the case of a clear violation to avoid silencing public debate.

BLOCK

Communicators should be mindful of the importance of respect and the right to freedom of expression! Disruptive activities may merit blocking a user from a specific platform. However, each case should be clearly motivated based on the platform's code of conduct.

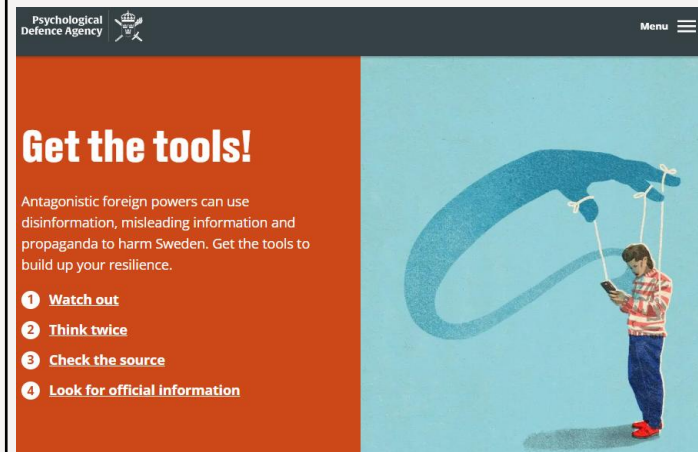
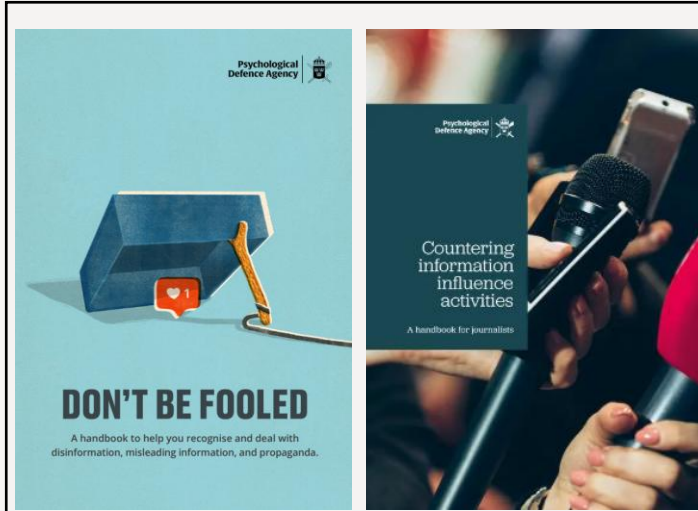
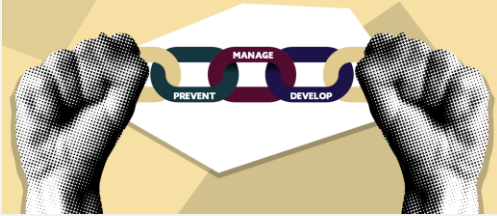
EXPOSE

Although generally not recommended, a strategic response to information influence activities could be exposing the actor behind, for example, a deceptive account. Again, this should not be done lightly. First conduct a proper consequence analysis that considers the consequences exposing the culprit could have for your own organisation, for your stakeholders, and for the person who will be exposed.

Advocacy-based response

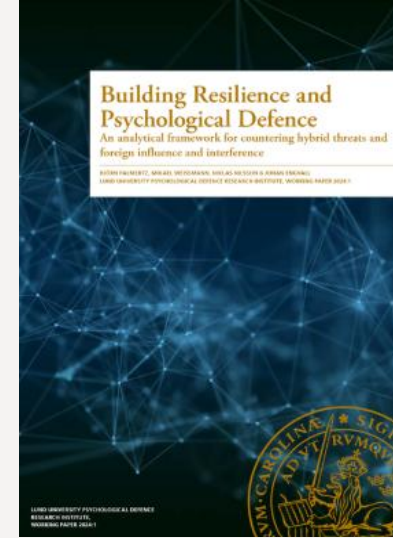
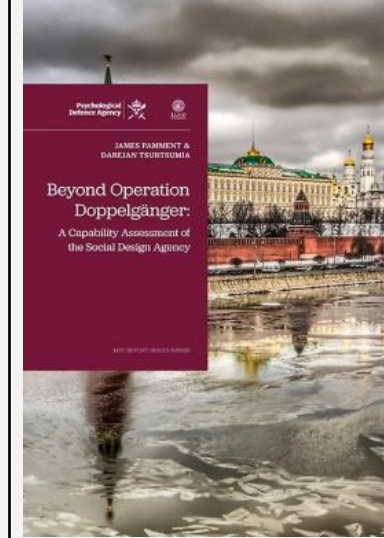
Trainings and online courses

THE CAPABILITY PLATFORM



Information material

Research and studies



Collaborations

Important information to all residents of Sweden

In case of crisis or war

To all residents of Sweden

We live in uncertain times. Armed conflicts are currently being waged in our corner of the world. Terrorism, cyber attacks, and disinformation campaigns are being used to undermine and influence us.

To resist these threats, we must stand united. If Sweden is attacked, everyone must do their part to defend Sweden's independence – and our democracy.

We build resilience every day, together with our loved ones, colleagues, friends, and neighbours. In this brochure, you learn how to prepare for, and act, in case of crisis or war.

You are part of Sweden's overall emergency preparedness.

Psychological defence

Foreign powers and others outside Sweden use disinformation, misinformation and propaganda to influence us.

Attempts to influence us, primarily through online platforms and social media, occur on a daily basis. The goal of these actions is to sow mistrust and erode our will to defend ourselves.

Those seeking to influence us may do so in the following ways:

- Spreading lies, false narratives, or stories that are partially true, but taken out of context.
- Manufacturing fake images, videos or voice recordings.
- Attempts to elicit strong emotions related to certain issues or events to heighten a sense of worry or suspicion towards each other.

How you can contribute to our collective resilience:

- Be mindful of content that elicits a strong reaction.
- Only share information you know comes from reliable sources.
- Try to verify information from several different sources.
- Get verification from official government sources when something serious has happened.

Psychological Defence Agency

