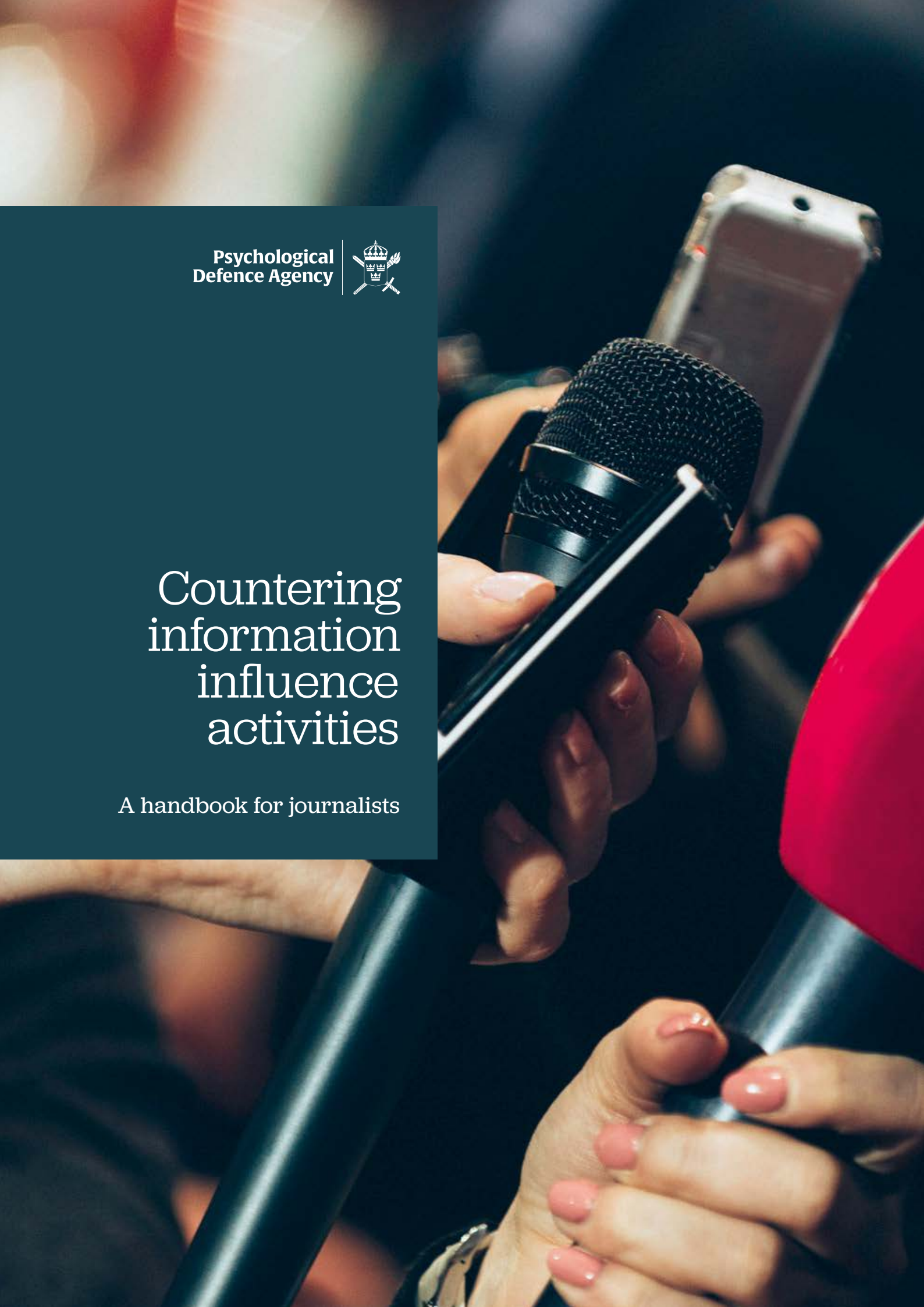
Psychological Defence Agency

Countering information influence activities

A handbook for journalists



COUNTERING INFORMATION INFLUENCE ACTIVITIES — A HANDBOOK FOR JOURNALISTS

Swedish Civil Contingencies Agency (MSB)
funded the production of the original document.

Photo: Microgen/iStock

Print: Brand Factory

Production: Familjen

Publication number: MPF/2023:521 -2

ISBN: 978-91-527-8749-6

Content

Introduction

Security threats today can assume a radically different character than what we usually associate with international conflict. In this type of conflict, actors generally use means other than military to achieve their goals. This new type of security threat is called an influence campaign. Foreign powers use influence campaigns to exploit societal vulnerabilities to achieve their goals without military force. We must defend ourselves against this phenomenon to safeguard democracy.

The handbook defines 'influence campaign' as a set of activities coordinated by a foreign power that involves the promotion of misleading or inaccurate information or other specially-adapted actions aimed at influencing the decisions of politicians or other public decision-makers, the opinions of all or a part of the population, and opinions or decisions taken in other countries. An influence campaign consists of a number of influence activities, one of which is information influence.

Using information to influence others is nothing new. Fields such as public relations and advertising use targeted information to influence the personal decisions of people around the world every day—to buy a particular brand or support a certain political candidate. As citizens, we expect such communication to follow certain rules. For example, communication should take place openly, be based on truthful and accurate information, and be presented in such a way as to allow us to make informed choices.

But not all agents of influence play by these rules. Information can be deployed covertly and deceptively by foreign powers to undermine critical democratic processes, control public dialogue, and influence decision making. These are what we refer to as information influence activities.

Psychological defence is the collective ability of society to resist foreign malign information influence activities and other disinformation. Many actors contribute to the psychological defence. Free and independent media is a key player along with agencies and institutions. By increasing knowledge and awareness regarding disinformation – its existence, how it is spread and can pose a threat, reduces the risk of malign influence affecting our society.

This handbook was originally created for communicators by the Swedish Civil Contingencies Agency in 2018 in response to the deteriorating security situation in the world. It is based on research from the Department of Strategic Communication at Lund University. It has been adapted for journalists and media organizations by the Psychological Defence Agency and the media institute Fojo at Linneaus University in Sweden.

This adapted version of the handbook will help you as a journalist or a media organization to become more aware of and resilient to information influence activities.

Part I | Becoming aware of information influence

What is information influence?

Open debate, differences of opinion, and seeking to persuade are essential features of a healthy democratic society. But what happens when someone fabricates evidence, provides fake 'experts', or makes deliberately misleading arguments? Such activities are damaging for society and problematic for democratic processes.

> **A suitable response to information influence is based on facts, evaluation of sources and the principles of free speech; it aims to defend our democratic society.**

Most democratic countries enjoy healthy, vibrant political debate where individual citizens, journalists, academics, and representatives of civil society who, beyond the important task of holding decision-makers to account, see it as their role to point out cases of overtly false or misleading information. State actors can support such efforts by providing funding in support of healthy civil engagement and by correcting inaccuracies related to their own work. This system has served liberal democracies well for centuries, at least in theory. However, the debates about fake news so prevalent today suggest that vulnerabilities in the system are now being exploited.

Furthering interests of foreign powers

Information influence activities involve potentially harmful forms of communication which are knowingly or unknowingly orchestrated by foreign state actors or their representatives. Information influence activities are used to further the interests of a foreign power through the exploitation of perceived vulnerabilities in society.

> **Foreign powers deliberately interfere in a country's internal affairs to create a climate of distrust between a state and its citizens. Foreign state actors study the controversies and challenges of a society and exploit these vulnerabilities to disrupt and polarise.**

Isolated incidents or extensive campaigns

Information influence activities can be carried out as isolated incidents or as part of a more extensive campaign seeking to exert influence. Influence campaigns use a wide range of techniques, including techniques drawn from the field of communications. In addition to communications tools, everything from diplomatic and economic sanctions to displays of military force can be used to exert influence on society.

Authenticity is difficult to determine

There is a certain ambiguity to these activities, which can make it hard to differentiate between information influence activities and genuine public debate. Political debates can be sensitive, uncomfortable, and sometimes even nasty. But they are part of the democratic process that relies on a plurality of opinions and the freedom to debate them. However, constructive debate cannot take place if hostile foreign powers introduce deliberately misleading information to disrupt and control.

> **It is important to remember that holding opinions similar to those of a foreign power does not automatically make that person an agent of that foreign power. When we talk about information influence activities, we are talking about the systematic use of deceptive techniques to undermine democracy. Such attempts to destroy democracy must be — countered by safeguarding our fundamental democratic principles — free and open debate, freedom of expression, and democratic dialogue. These should always be the cornerstone of our response to information influence activities, even if it makes the task more difficult. This cannot be emphasised enough.**

Techniques for deception

Public relations, marketing, diplomacy, opinion journalism, and lobbying are examples of accepted ways of influencing people's views and behaviours. Information influence activities mimic these forms of engagement but use the techniques deceptively.

Disrupting public debate

Foreign powers use information activities to influence those fields and debates from which they can benefit. This can be done both directly and indirectly, through everything from open propaganda to covert funding of civil society groups. When illegitimate actors interfere in legitimate public debate it can change society's perception of leading opinions and influence decision-making.

Acting in self-interest

Influence activities are intended to achieve specific goals that benefit a foreign power. The objective might be anything from destabilising a society politically, preventing specific decisions from being taken, or polarising a political debate.

Exploiting vulnerabilities

All societies have their challenges. These may be social or class tensions, inequality, corruption, security issues, or other problems central to social life. Hostile foreign powers identify and systematically exploit these vulnerabilities to achieve their goals.

Various exploitable vulnerabilities

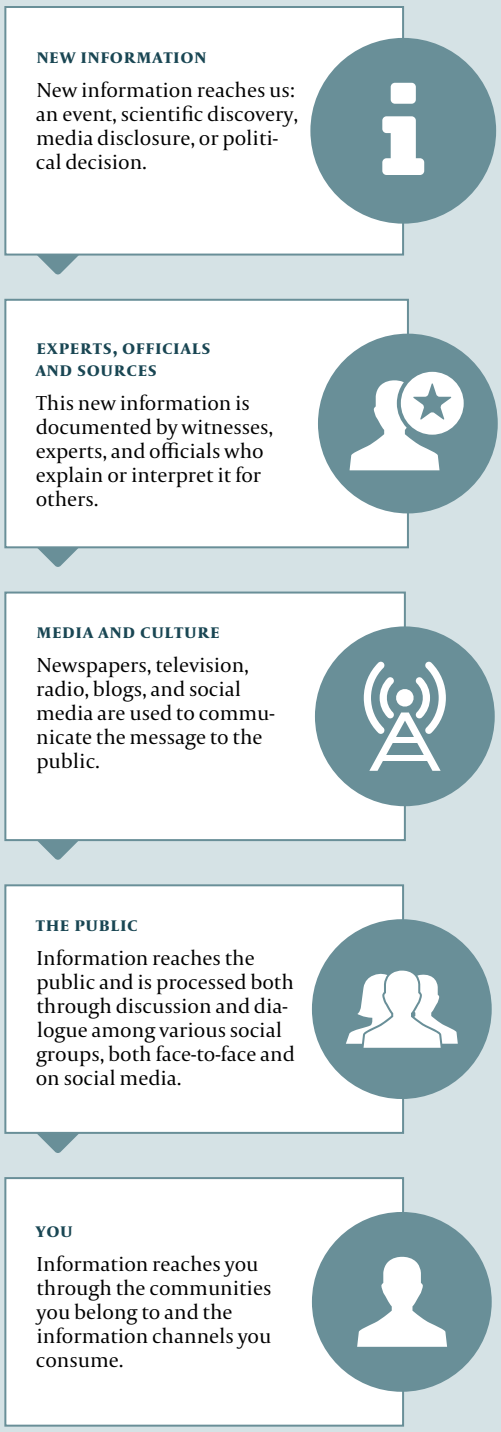
Let's imagine that our opinions arise as the result of a rational process: Something happens, or a new piece of information comes to light. Witnesses, researchers, government officials, and others with credible expertise interpret or explain the situation within a larger context. The media pick up this information and spread it to various communities, online and offline, which is how it comes to you. Of course, in practice it may differ somewhat, but in broad strokes this is the theory of how opinions are formed in a democratic society.

The process is based on a few simple principles: Information about the original event must be genuine and based on facts. Claims must be verified by credible sources who are indeed real people with a reputation to lose if they distort the truth. The media reporting on the story must be balanced in their presentation, double-check facts and sources, and strive to serve the public interest. Deliberative communities weigh differences of opinion and engage in productive debates before reaching reasoned conclusions.

> **Information influence activities are geared towards exploiting the various ways in which the ideal of rational deliberation is at odds with reality. Hostile actors use creative, opportunistic, and technologically advanced influence techniques to insert themselves into these steps to corrupt the flow of information. They identify vulnerabilities in how we form our opinions, how critical information travels through the media landscape, and how our brains process information.**

Evidence can be forged or manipulated, experts may not be experts at all, and witnesses can be bribed or coerced. News services can be run as one-sided propaganda channels and the public debate online can be conducted between automated bots to create the illusion of a lively public debate. When these activities are carried out deliberately, through coordinated campaigns aimed at undermining the democratic process, we cannot always rely on the system to self-correct.

Opinion formation



MEDIA SYSTEM VULNERABILITIES

Our modern media system has a number of vulnerabilities, especially rapidly evolving technologies, changes to the journalistic business model, and the proliferation of alternative news sources. With everything from forged letters and photoshopped images, to algorithms, bots, and the competition for clicks on social media, the media system is vulnerable to those who want to exploit it for their own benefit — for political or economic gain, or just to see if it can be done.

PUBLIC OPINION VULNERABILITIES

Public opinion formation has always been vulnerable to certain phenomena such as social proof — i.e. copying the behaviour of others interpreted as being 'correct' or desirable. But in today's information environment, where social media accounts can be faked and armies of trolls pollute comment fields, it is easier than ever to fabricate evidence, arouse anger, and provoke outrage. All this makes public opinion formation vulnerable to deliberate manipulation.

COGNITIVE VULNERABILITIES

Some vulnerabilities are the result of how our brains are wired: While we aren't designed to cope with all of the information we are exposed to in the modern world, our personal data can be leveraged through psychographic analysis to know us better than we know ourselves. Estimates suggest that there are many as 800 data points on every individual using social media that can be used to predict almost everything about you. Information influence activities exploit our thought patterns to exert influence over our perceptions, behaviours, and decision-making.

Differences between information influence and communication?

To identify cases of information influence, you must assess the extent to which communications are misleading and are intended to harm and cause disruption. Weigh these factors when considering a suspected influence activity to make an informed decision as to how to construct your response. The goals and motivations behind influence activities may not be readily apparent. However, the greater the number of such factors you identify, the higher the probability you are dealing with a case of information influence.

> **It is no coincidence that techniques employed in information influence activities often overlap with journalism, public affairs, public diplomacy, lobbying, and public relations — copying legitimate methods is one of the ways to disguise information influence activities and make them appear to be providing reliable information. Please note that illegal influence activities, such as threats, hacking, blackmail, and bribery, are outside of the scope of this discussion and should be reported to the police.**

Deceptive

Reliable communication is open and transparent. The content is credible and can be verified. Information influence activities are deliberately misleading.

Intentional

Reliable communication contributes to constructive debate, even if the arguments or content may be controversial. Information influence activities are intended to undermine constructive conversation and hamper open debate.

Disruptive

Reliable communication is a natural aspect of our society that strengthens democracy, although it sometimes creates friction. Information influence activities disrupt democratic dialogue and weaken the functioning of society.

Questions for journalists to consider

- What motives might exist in a conflict and how should they be taken into considereation before publication?
- What role do you think the media should serve in the present information environment?
- How might journalism strengthen democratic discourse?
- What happens to journalistic credibility when journalists themselves are deceived by fake accounts or documents?
- How might the media investigate the influencing of public opinion (including any hidden agendas) that takes place on social media, e.g., when 'filter bubbles' determine which voices are heard?

Part II | Identifying information influence

Information influence techniques and strategies

Two strategies for information influence

To identify information influence activities, you first must recognise the two general strategies used:

- Strategic narratives
- Target audience analysis

Knowing these can help you to recognise information influence activities as well as understand their aims.

Strategic narratives – stories with an objective

Information influence activities usually involve storytelling of some kind. The portrayal an event, issue, organisation, place, or group is generally formulated to fit into a pre-existing narrative. For example, most people have heard of the Space Race between the United States and the Soviet Union during the Cold War. And most people know something about how we sent men to the moon as well as rumours that the moon landings were faked. There is a video showing an astronaut planting a flag on the moon. While some will take this as evidence that it happened, others claim the video is a fake. These narratives are typical of the 'knowledge' we unconsciously use to sort new information. When we hear new stories about space travel, we sort them according to which of these narratives we believe. When such stories are deliberately planned and used in communication activities they are known as strategic narratives.

For example, one might invent something about a certain religious or ethnic group that fits in with what people already believe about these groups, i.e. the existing narrative. Disinformation can affect us in three different ways —

- by highlighting some aspect of an existing narrative,
- by suppressing some aspect of it,
- by linking the narrative to unrelated events in order to distract.

Identifying the strategic narratives at play and the logic behind them is an important step in devising an appropriate response

Positive or constructive: "This is the truth!"

Tries to establish a coherent narrative about a particular issue that fits into, complements, or expands upon existing, well-established strategic narratives.

Negative or disruptive: "This is a lie!"

Attempts to prevent the emergence of a coherent narrative, or to disprove or undermine an existing narrative.

Distraction: "Look over here!"

Diverts attention from key issues by means of e.g. humour, memes, or conspiracy theories

Target audience analysis

Analysing strategic narratives is one approach to identifying the logic behind an information influence campaign. A second, connected approach is to consider for whom these strategic narratives resonate — what is the target audience?

- Are the narratives meant for the general public, or are they aimed at a specific group?
- Is 'big data' being used to target individuals with particular personality traits or sentiments?
- If some form of targeting is taking place, is the focus on groups or individuals with specific vulnerabilities or patterns of behaviour?

Understanding who is being targeted using which narratives is an important step in assessing the severity of the specific case at hand.

The general public: widest possible audience

Information influence activities target society as a whole by aligning messages with widely shared narratives.

Sociodemographic targeting: specific groups

By identifying audiences based on demographic factors such as age, income, education, and ethnicity, messages can be tailored to appeal to a specific group.

Psychographic targeting: individuals

By analysing and categorising big data, influence activities can target individuals with specific personality traits, political preferences, patterns of behaviour, or other identifying features

Information influence techniques

Information influence activities use a range of techniques to influence people's lives. Information influence activities are continuously evolving. However, by studying a wide variety of examples, we have abstracted six common techniques that you should be on the lookout for. Sub-techniques are characterised by similar principles within each group. Awareness of how these techniques look and work will help you to recognise them.

In most cases, the techniques are neutral — neither good nor bad in themselves. They can be used in open and accepted ways as a natural part of the democratic dialogue, or with a deceptive and hostile intent as part of an information influence campaign. The use of any one technique is not necessarily a sign of information influence.

You should instead assess the degree to which the activity is intentionally misleading with the aim of harming society, and, additionally, analyse the use of these techniques in conjunction with an assessment of strategic narratives and target groups:

- How strong are the indicators of misleading or disruptive intent?
- What do the strategic narratives and target audiences suggest about the purpose of the communications?
- If a specific technique is being used, could it be harmful to the public or to our society?

Information influence techniques

SOCIAL AND COGNITIVE HACKING

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

DECEPTIVE IDENTITIES

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

SYMBOLIC ACTIONS

- Leaking
- Hacking
- Public demonstrations

MALICIOUS RHETORIC

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

DESINFORMATION

- Fabrication
- Manipulation
- Misappropriation
- Satire and parody

TECHNICAL EXPLOITATION

- Bots
- Sockpuppets
- Deepfakes
- Phishing

Social and cognitive hacking

Social and cognitive hacking refers to activities that exploit our social relationships and thought processes. It is similar to hacking a computer in the sense that hostile actors seek to trick, or 'hack', these processes by exploiting vulnerabilities. For example, we usually prefer to fit in with what people who resemble us think and do, and it can be difficult to think rationally when we are exposed to emotionally loaded material. These predictable patterns of behaviour can be exploited by hostile actors who deliberately trigger our vulnerabilities, for example in social debates on sensitive issues, to achieve their goals.

Table 1. Glossary.

Techniques for social and cognitive hacking	
Dark ads	Messages tailored to an individuals' psychographic profile are considered dark ads. Data gleaned from social media and other sources can be organised into a database of individuals with a similar ideological opinions and personality traits. Advertisements that are only shown to certain individuals can include messages that appeal to their psychological leanings and encourage certain behaviours.
Bandwagon effect	People who feel they belong to the majority are more likely to voice their opinions. Bots can boost the number of likes, comments, and shares of a social media post to give the impression of social acceptance. This appeals to the cognitive need for belonging and facilitates further engagement from actual human users.
Spiral of silence	People who feel they belong to the minority are less likely to voice their opinions. Contrary to the bandwagon-effect, the appearance of social conformity around an issue can cause people with minority opinions to remain silent. This plays on the fear of being excluded or singled-out because of an unpopular opinion
Echo chambers and filter bubbles	Organic sub-groups in which people communicate primarily with others who hold similar opinions 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, more significantly, socialise with each other. Thus, they are rarely exposed to ideologically different opinions. This can be exploited online to spread targeted information to specific groups.

Deceptive identities

We often evaluate the credibility of information by looking at its source. Who is communicating with me and why? What do they know about the issue? Are they who they claim to be? By imitating legitimate sources of information (be they persons, organisations, or platforms), hostile actors engaged in information influence activities exploit the 'trust capital' accrued by legitimate sources through the use of fraudulent identities.

Table 2. Glossary.

Techniques for deceptive identities	
Shilling	A shill is someone who gives the impression of being independent but, in reality, works in partnership with somebody else or receives payment to represent them. Examples include paid reviewers of products on shopping websites, audience members employed to applaud a speaker during a public meeting, or a group of online trolls paid to write negative comments.
Imposters and con-artists	Imposters pretend to be someone they are not, i.e. they adopt the personal or professional identity of another person. Con-artists claim to have expertise or credentials they lack, e.g. someone who falsely claims to be a medical doctor or a lawyer without having undergone the required training.
Counterfeits	Fabricating official documents is an effective way of making disinformation appear authentic. For example, fake letterheads, stamps, and signatures can be used to produce forged documentation.
Potemkin villages	Malicious actors with sufficient resources can set up fake institutions and networks that serve to deceive and mislead. Potemkin villages are false companies, research institutions, or think tanks created to authenticate or 'legitimise' targeted disinformation.
Fake Media	Disinformation can also be circulated by creating fake media platforms that look like, or that have a web address similar to, a real news site. It is relatively easy and inexpensive to create a fake website online that looks almost identical to a real website but publishes very different content.

Recognize deceptive identities

URL

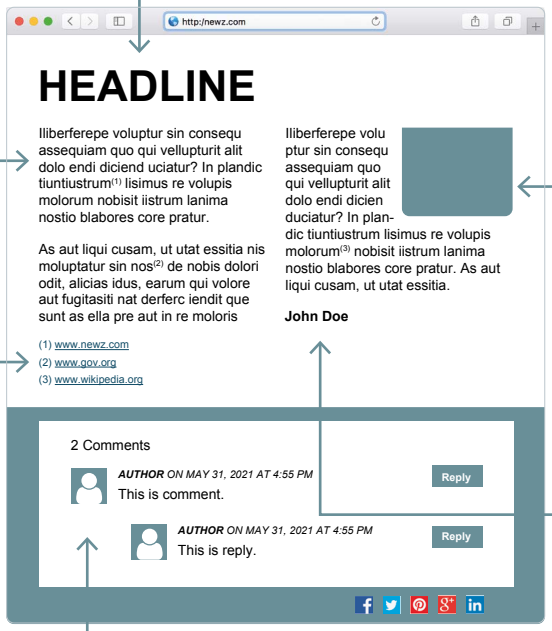
Imitating well-known platforms to gain legitimacy is a common information influence technique. Make sure you are on the right platform by taking a closer look at the URL.

HEADLINE

Headlines aspire to generate interest and a response from the reader. Keep reading beyond the headline to make sure that it matches the content of the article.

CONTENT

Assess the content of the text. Is it informative, argumentative, based on facts, emotions, or opinions? Always read the entire text before sharing.



IMAGES

Images do not always reflect reality. Images can be manipulated easily by deleting, editing, or adding elements. They may not even be connected to the story. Use image search to find out if an image has been used before in another context.

SOURCES

If the text refers to other sources, check the links to trace the origin of the information. Assess whether or not it has been used appropriately.

AUTHOR

Be wary of articles with no by-line. If the author is given, consider who that person is and the reason behind the article.

COMMENTS

Comments on webpages and in social media most often come from ordinary people expressing their opinions. But some comments may also be posted by trolls and bots. Consider who is making comments.

ENGAGEMENT

Just because a text has been liked or shared a lot does not mean that the content is correct. Be wary of sharing content simply based on the appearance of engagement by others.

Symbolic actions

Actions speak louder than words. Some actions are calculated to convey a message, rather than to achieve the objective of the action itself. In such cases, the action is symbolic. In contrast to any ordinary actions, symbolic actions are motivated by a communicative logic and a strategic narrative framing. This can be done very crudely, for example the way terrorists do by playing on universally shared fears of random violence. It can also be done in a sophisticated manner by using precise cultural symbols relevant only to a specific target audience.

Table 3. Glossary.

Techniques for symbolic actions	
Leaking	Leaking consists of releasing information that has been obtained by illegitimate means. This carries symbolic weight as leakers traditionally reveal injustices and cover-ups unknown to the public. However, when used as an information influence activity, leaked information is taken out of context and is used to discredit actors and distort the information environment. Leaked information is sometimes obtained through hacking or theft.
Hacking	Hacking involves acquiring unauthorized access to a computer or a network and is a crime. Hacking as an information influence activity, can serve as a symbolic act where the intrusion itself is secondary. The actual objective is to arouse suspicion that a system is insecure or compromised, in order to undermine confidence in the system in question or a body responsible for the same.
Public demonstrations	Legitimate demonstrations are symbolic actions used to promote a certain political issue or position. They are an important element of the democratic dialogue. Hostile actors, however, may orchestrate demonstrations to falsely give the impression of strong support or dislike of a particular issue (also known as astroturfing).

Malicious rhetoric

Rhetoric is an accepted and natural part of democratic debate where everyone has the right to voice their opinions and engage in public deliberation. A certain amount of rhetoric is accepted in public debate whereas malicious rhetoric is not. Malicious rhetoric exploits the often-fragmented nature of public conversations to muddy the waters, deceive and mislead, and discourage certain actors from participating in the public debate.

A common vehicle for malicious rhetoric online is the troll. Trolls are social media users who deliberately provoke others through their comments and behaviour online. Their activity contributes to increased polarization, silences dissenting opinions, and drowns out legitimate discussion. Trolls may be driven by personal motivations or, as in the case of hybrid trolls, work under the direction of someone else.

Table 4. Glossary.

Techniques for malicious rhetoric	
Ad hominem	Attacking, discrediting, or ridiculing the person behind an argument instead of the argument itself is called an ad hominem attack. This is done to silence, deter, or discourage one's opponent.
Whataboutism	Deflecting criticism by drawing false parallels with similar, yet irrelevant phenomenon.
Gish-gallop	Overwhelming an opponent with a flood of arguments, facts, and sources, many of which are spurious or unrelated to the issue.
Strawman	Discrediting an adversary by attributing positions or arguments to them that they do not hold and then arguing against those positions.
Hijacking	Taking over an existing debate and changing its purpose or topic. This is particularly effective when applied to hashtags and memes, and may also be used to disrupt events or counter-cultural social movements.

Disinformation

Disinformation refers to erroneous or manipulated information that is deliberately disseminated in order to mislead. This is the cornerstone of classic propaganda, but it is also the basis of the more recent phenomenon of fake news.

> **The deliberate use of false information to mislead is nothing new. However, digital platforms have fundamentally changed the nature of disinformation.**

Spurious content can occur in the form of manipulated text, image, video, or audio. These elements can be used to support false narratives, sow confusion, and discredit legitimate information, individuals, and organisations.

Table 5. Glossary.

Techniques for disinformation	
Fabrication	Information with no factual basis published in a style that misleads the audience to believe it to be legitimate. For example, a fake e-mail from a politician might be produced and leaked to the press to undermine that politician's credibility.
Manipulation	Adding, removing, or changing the content of text, photo, video, or audio recording to communicate a different message.
Misappropriation	The use of factually correct content presented on an unrelated matter to frame an issue, event or person in a deceptive way. For example, a false news article might use pictures from an unrelated event as proof of its existence.
Satire and parody	Satire and parody are normally harmless forms of entertainment. However, humour can be used aggressively to disseminate misleading information and ridicule or criticise individuals, narratives or opinions. Humour can also be a very effective way of legitimising controversial opinions.

Technical manipulation

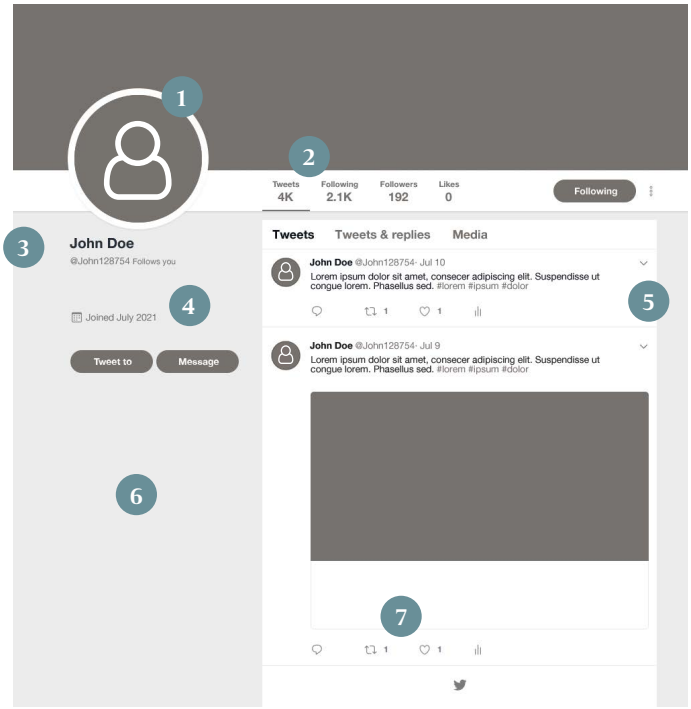
Information influence activities often take advantage of the latest technologies. Malicious actors use advanced technical skills to manipulate flows of information online through automated accounts and algorithms, or through a combination of human and technological approaches. Note that new techniques are often used to perform traditional information influence activities such as creating deceptive identities or spreading disinformation. This is an area that develops much more quickly than our ability to analyse and understand its potential uses and consequences. Recently developments regarding 'deepfakes', machine learning, and artificial intelligence have been highlighted in public debate, and we can expect that such tools will be increasingly utilised for information influence purposes in the future.

Table 6. Glossary.

Techniques for technical manipulation	
Bots	Bots are computer programs that perform automated tasks, such as sharing certain types of information on social media or answering FAQs on customer service platforms. However, they can also be used to emphasise particular messages online, to spam discussion forums and comments, to like and share posts on social media, and to implement cyber-attacks.
Sockpuppets	Imposter accounts managed by someone who does not reveal their real identity or intentions are called sock-puppet accounts. Such false identities are used to join online communities and participate in debates to introducing false or controversial information. Two or more sockpuppets can be used in conjunction to artificially simulate both sides of a debate.
Deepfakes	Advanced machine learning algorithms can now be used to manipulate audio and video very convincingly, for example of a real politician delivering a fictitious speech. It is even possible to superimpose the face of another person onto pre-existing video footage and digitally reconstruct a person's voice.
Phishing	Phishing is a technique that tricks users into revealing their passwords or other sensitive information online. Phishing involves automated spamming of emails that look legitimate but actually lead to fake websites that harvest any personal information entered. Spear Phishing is a more sophisticated type of phishing used to access information on secure computer systems.

Spot the bot

While bots are efficient tools of influence on social media, they are also vulnerable to exposure. Verifying the following seven features can help you to spot a bot online. But be on your guard — different types of bots can look very different. Impersonator bots are designed to look like real users. Spambots, on the other hand, focus on disseminating large volumes of information, and often lack natural user characteristics.



1 PROFILE PICTURE

Bots usually either lack a profile picture or use a stolen one. Use image search to verify the authenticity of suspicious profile pictures.

2 ACTIVITY

Spambots tend to be highly active, sometimes generating more than 50 each day. Look out for accounts with a suspiciously high number of posts per day.

3 NAME

Most bots generate their user names automatically. Usernames consisting of seemingly random letters and numbers may be bots.

4 CREATION DATE

Most bot accounts are created for purpose and so have no user history. Sometimes older accounts are hacked and re-purposed, removing old posts. Consequently, such accounts have wide gaps between intense periods of activity.

5 LANGUAGE

Bots sometimes use automatic translation to spread messages in multiple languages. This results in obvious grammatical errors or incoherent sentences. Accounts that publish similar content in multiple languages may be bots.

6 INFORMATION

Bot accounts are created to operate anonymously, so they lack personal information, or use fictional or forged information. Verify any information provided.

7 ENGAGEMENT

Review which posts a suspicious account engages with. Bots are often coordinated and reinforce messages spread by other bots. They are not likely to have real followers.

Combinations of information influence techniques

To identify a case of information influence, you must assess the strategic narratives, target audiences, and communication techniques used. Remember that malicious communication techniques are often deployed in combination to support and reinforce one another.

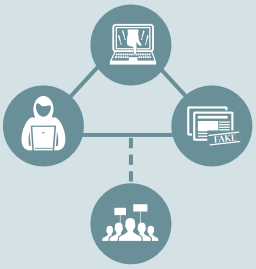
For example, a forged document will reach a wider audience if spread by bots. The effect will be more widely amplified if coordinated with articles published on biased or fake news platforms supported by a troll army of commentators.

Coordinated techniques

Information influence operations are often complex, and you will rarely encounter a single technique in isolation. Be on the lookout for a combination of techniques directed against you. While theoretically the possible combinations are infinite, it is worth noting some common combinations.

POLARISATION

Polarisation exacerbates opposing extremes on a specific issue. This strategy may use social hacking, deceptive identities, and disinformation. Trolls and bots are often used to reinforce extreme opinions.

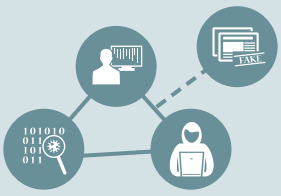


LAUNDERING

Laundering refers to gradually distorting and de-contextualizing information, so that it becomes impossible to tell if its source is true or false. This strategy may use deceptive identities, disinformation, technical manipulation, and symbolic acts in combination with social and cognitive hacking to create a web of false information.

PROVOCATION

Provocation exploits sensitive issues to antagonise people and to generate anger and discord. This strategy may use social and cognitive hacking, deceptive identities, and malicious rhetoric to engage ordinary citizens by exploiting their emotional vulnerabilities.



FLOODING

Flooding creates confusion by overloading audiences with information, either positive, negative or irrelevant.

This can be done by spamming and trolling on social media, or by disseminating disinformation to legitimate media sources. Flooding crowds out legitimate information and discourages constructive debate.

Considerations for journalists when evaluating material

- What narratives can you identify and who are they aimed at?
- Is there any evidence of an intention to deceive or disrupt public discourse?
- Do you suspect interference from a foreign actor or proxy?
- Do you see a combination of techniques suggesting a coordinated effort or campaign?
- Do you have tools to check the authenticity of the tools?

Part III | Countering information influence

Advice and strategies for countering information influence activities

For journalists, there are several aspects to countering information influence. A media outlet can be attacked as an organisation or business, in the same way as goverment agecies, with regards to disinformation efforts, social media hacks, and the like. Such information influence activities are seldom addressed by journalists but are rather handled by the organisation in which they work, preferably on the basis of a strategy. At the same time, the organisation's handling of such activities impacts the work of journalists. The craft of journalism, for example, could be improved by drawing lessons from organisational responses to influence activities. For that reason, this part of the handbook includes advice for organisations managing information influence activities as well as advice for journalists. The advice to organisations is primarily directed at the communications officers, marketing departments, etc. of media outlets. Media outlets which suspect that they are the target of an information influence campaign can, as of 1 January 2022, contact the Swedish Psychological Defence Agency. The agency, is tasked with providing advice and support to affected media actors. The section on journalism is not included in the handbook for communicators. This section draws on research and reports from the UK-based non-profit First Draft (2015–2022), which has long been a leader in supporting journalists and media outlets in the fight against disinformation. Reports, guidelines and advice from international organisations such as Africa Check and the EU's East StratCom have also been reviewed. The end of the section includes summarised advice on hostility and threats directed at journalists.

Such threats are closely related to disinformation and information influence activities, and they often occur in tandem. Those wishing to learn more are directed to specialised information and the helpdesk available from Demokratijouren at Fojo. These are available on Fojo's website.

Organisational advice

Prepare and protect

The preparations you make in advance for information influence activities are the most important part of preparedness. Educating your co-workers and establishing response structures makes it possible to mitigate the negative effects of information influence operations and to respond quickly and efficiently. Preparation consists of three main phases:

- sharing information and raising awareness,
- understanding of how your key audiences and stakeholders may be vulnerable to information influence activities and developing narratives and messages around potential problems, and
- carrying out a risk and vulnerability analysis for your organisation.

Creating awareness

The first step toward dealing with a problem is recognising that the problem exists, therefore an essential aspect of preparedness is raising awareness of the threats we face as a society, and of the issues that can be considered vulnerabilities for your organisation in particular. At the level of society in general, the best defence against information influence activities is to develop the capacity to handle threats by creating cross-sector platforms where leaders, journalists, representatives of social media platforms, researchers, communication professionals, and citizens can exchange knowledge and best practice lessons with each other and with the general public.

There are several things that individual media outlets can do to help build resilience and defensive capacity within your organisation. First, you can put yourself forward as a key point of contact for these issues within your organisation. It is essential to discuss these issues with senior management and to communicate internally with your colleagues. Second, you can act as an advisor for your managers and colleagues, so they know what to do if faced with information influence activities. This includes identifying needs and training opportunities. Third, you can build networks with other professionals outside of your organisation based on mutual support and exchange of experiences. Fourth, you can increase awareness and transparency regarding the activities of your media outlet to prevent the spread of disinformation.

> **Start building a network within your media outlet and with other media outlets for mutual support and exchange of experiences.**

Building trust through strategic communication

One of the goals of information influence is to undermine trust between people and social institutions such as many legacy media represent. Therefore, the effect of these activities can be minimised by focusing on countermeasures that build trust in your organisation. Supporting the reputation and legitimacy of your organisation is an important aspect of any counter measure strategy.

> **One of the goals of information influence is to undermine trust between people and social institutions such as many legacy media represent, the effect of these activities can be minimised by focusing on countermeasures that build trust in the organisation.**

In the heat of the moment, it can be difficult to get the right message across. That is why it is vital to prepare the message that you will communicate. The messages should assert your organisation's values, and can be readily adapted to a specific event. Just as you use targeted messages to describe a new initiative, product or news story, you can also use messages to raise awareness of fake stories and to refute them.

When designing messaging, it is important to consider which stories are in circulation about your organisation and what are the overarching narratives that drive these stories. The narratives will be linked to the way in which your organisation is perceived by different audiences. How do individual messages contribute to the identity, values, and narratives your organisation wishes to project, particularly in relation to different key audiences? Messaging that supports positive narratives about your organisation can play a crucial role in developing resilience to misleading and false information.

> **The organisation's response is limited by the fact that they are always responding to someone else's agenda. The attacker seems to set the terms, making the entire principle of responding to information influence activities problematic. It often feels like, while the one exerting information influence acts, you react, meaning that you are always one step behind them.**

Therefore, it may be wiser to focus on efforts that defend democratic values such as free debate and freedom of expression, which is generally also the core and driving force of media outlets. Journalism should safeguard and protect opinion formation, and it can do so by minimising the impact of vulnerabilities in media, opinion and human thought. In this respect, it is important to have a strategic, well-considered response that is also based in facts. It bears repeating that efforts to counter information influence may not lead to a silencing of public debate. That would defeat the very purpose of responding to the information influence activities, encourage polarisation and help undermine the functioning of society. Open and democratic debate must always be protected and encouraged.

Know your organisation's narrative and target audience

A strong organisational narrative comes from a clear set of values and objectives within the organisation. Messages sent should align with the overall narrative that the organisation seeks to communicate. By analysing and seeking to understand the factors that contribute to the narratives your media outlet wishes to convey, you create an understanding of your organisation's vulnerabilities. Attacks in the form of information influence are best countered by maintaining and upholding the values your media outlet stands for. Get to know your audience to understand where they are most vulnerable to information influence activities. For example, certain age groups or those living in a certain location may be particularly vulnerable. You should prioritise those who are most vulnerable when preparing a message. A network of key communicators may also be needed to help reach the most vulnerable audiences. There are experts available for target audience analysis. Such an analysis can help mitigate damage if your media outlet is subject to information influence attacks.

Know your media outlet's risks and vulnerabilities

In addition to awareness, exchange of experiences and knowing your organisation's narrative and target audience, you should assess the threat posed by information influence activities to your media outlet's operation. Such an analysis can be made as follows:

Step 1: Point of departure. What role does your organisation play and what are its responsibilities? Which methods can be used to identify and evaluate risks and threats? What frameworks or perspectives will you use in your analysis?

Step 2: Risk assessment. What are the possible threats and risks? What is the likelihood of these events taking place, and what are the possible consequences? Which situations should be assessed regarding your organisation's crisis management capabilities? What preventative measures should be taken?

Step 3: Vulnerability assessment. How might your organisation be affected by different scenarios? What are the potential consequences of information influence activities for your organisation, and how can you manage, resist, and recover from these consequences

Customise responses and counterstrategies

There is no ready-made solution to address all information influence activities. Information influence activities takes different forms, and the vulnerabilities and conditions of each media outlet are different. That's why it's important to customise your response. With thorough preparation, you can create an overall framework for appropriate counterstrategies that are suitable for the conditions and which can be adapted to the specific situation. An appropriate response should be in proportion to the gravity of the situation. The MSB proposes four different levels of response, each level suggesting specified methods:

1. Assess the situation.
2. Inform.
3. Advocate.
4. Defend.

The first level of response is to assess the situation. This is a neutral response that signals you are aware of the issue and are ascertaining the facts. The second level is to inform the public and key stakeholders about the situation and how your media outlet sees it. This is a slightly less neutral response that outlines what you consider to be the facts of the case.

The third level of response involves communicative actions that advocate a certain position. This means that you will actively argue your case, using rhetorical persuasion and public relations techniques to argue against, for example, disinformation. The fourth level is to actively defend your media outlet by taking specific actions against the aggressor.

Fact-based versus argumentative responses

If false information is allowed to circulate without being corrected, it can contribute to inaccurate perceptions of your media outlet, target audience or working methods. Therefore, your first action should always be response levels 1 and 2, to assess the situation and inform the identified target audiences. This is the starting point for a so-called fact-based response, which can be applied in most cases of suspected information influence activities. Consider how the false information might affect the media outlet and its operations. Try to find out who is disseminating the information, how widespread it is and what topic(s) are involved. Systematise collection. If false information is spread, the first step can be to respond with a correction. According to many experts, disinformation is best addressed by providing accurate information, while others argue that a corrected message only reaches those interested in learning the truth. The organisation's preparatory work on target audiences and narratives helps in assessing what action is appropriate in a given case. Response levels 3 and 4, advocating and defending, are argumentative. Such responses should be used sparingly but may be necessary in particularly serious situations. In such cases, the management of the media outlet should be involved in the process. Also ensure that any measures are compatible with democratic principles, freedom of expression and other regulations, such as the media outlet's rules on social media.

A fact-based response

The first two levels for counteracting influence activities are to assess and inform. They are applicable to most situations and constitute a fact-based response.

The examples below are suggestions for how to respond at each level.

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.

An advocacy-based response

Det tredje och fjärde steget i att bemöta informationspåverkan är att förespråka och försvara. Dessa steg innehåller åtgärder som bara är lämpliga i mer allvarliga situationer, där det tydligt går att identifiera informationspåverkan. Tillsammans är stegen det som kallas argumentbaserad respons.

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.

Proactive social media engagement

Social media are not just platforms where users can easily engage with each other, they can also be used as a tool for information influence. Social media platforms have their own logic. Users must understand and respect this logic to successfully counter information influence activities.

It can difficult to know who is behind a social media account and where they get their information. Individuals, forums, and networks may falsely claim to represent genuine public opinion. Social media are a challenge environment as information can spread rapidly, and elements such as *tagging*, *notifications*, *links*, and *attachments* must be considered. A typical social media post will contain one or more of these elements, which together contribute to positioning the post within a network of other accounts, ideas, and debates. Each post can be considered a part of one or several ongoing online conversations.

Countering influence on social media

The four levels of response provided above suggest a general approach to countering influence activities. Below is one example of how you could use this method to counter information influence on social media.

Assess. Assess the situation using your knowledge of information influence campaigns. Is it a case of information influence or just concerned citizens engaging in debate? If you suspect illegitimate influence, map the situation as clearly as possible. Which users are engaging with you? Are they hostile actors or are they reacting to provocation? Which hashtags are used? Are any links or visual materials attached? A quick assessment of the situation will allow you to determine the best line of action.

Inform. Design your message based on the conclusions you reached in your assessment. Carefully select which users, hashtags, and audiences to engage with. Focus on clarifying your position and assert your organisation's values using established and appropriate channels.

Advocate. If appropriate to the situation, assert yourself in the debate more clearly by advocating your position using tools available to you, such as prepared messages or multimedia. At this stage it may also be appropriate to involve yourself more in the debate to create greater engagement with the issue among your key audiences. This is done by communicating directly with other users to involve them in the issue.

Defend. Has the situation reached a point where productive dialogue is impossible and legitimate messages are being crowded out by spam and hostile content?

Depending on your organisational guidelines and the social media platform's code of conduct, you may have the right to block or ignore certain users. Take the advice from your leadership before acting! Freedom of expression is one of the core values of our society and we should always do whatever possible to maintain a free and open democratic dialogue. If you decide to block or ignore a user, be sure to be transparent about the reason for your decision.

Learn from experience

Collecting and documenting examples of information influence is central to better understanding the activities and ensuring an improved response in the future. A log of the event, including information about actions and dates, is one way of documenting what occurred. The log can later be used as a starting point when designing procedures and working methods against information influence activities in the future.

This knowledge can also be used to develop training materials and to improve organisational and societal preparedness. If society as a whole is to effectively counteract information influence activities, everyone must share their experiences and learn from each other. This applies both internally within an organisation and externally. From whom can your media outlet learn: other media outlets, civil society or public authorities?

Information to be logged

- Describe the background, course and context of the event.
- Who was involved?
- What characteristics did the information influence have?
- Were any vulnerabilities exploited?
- What techniques were used?
- Which target groups and narratives were used?
- Consider what effect the attacker sought to achieve, and justify your conclusions. How did you act?
- Also reflect on your choice of actions. What effect did they have? What might have happened if you had not acted?
- Also save evidence such as screenshots.

Advice for journalists

The internet in general, and social media in particular, have become a major part of most people's lives. Therefore, it is reasonable to expect of journalists that they monitor social media and understand how it works. This helps to prevent that you yourself spread disinformation, or that you or your media outlet are exploited by an influence campaign.

In this section you can read about journalistic fact-checking, which is used to verify published material — including on social media. The content is based on various reports by the global non-profit First Draft. First Draft's studies have long been highly influential in this field. The principles and methods described are also those used by organisations approved by and affiliated with the International Fact Checking Network (IFCN). Moreover, publications in the journalistic genre of fact-checking are fully transparent and readers can follow every step of the verification process and learn for themselves how to verify.

Journalistic fact-checking

Fact-checking is divided into two main branches:

1. **Scrutinising viral social media content.** This can range from fake competitions and advertising to posts about cancelled religious festivities and missing persons. Those carrying out influence campaigns look for cracks and conflicts in society, so such content is likely an attempt to influence, even if the post does not seem to have anything to do with information influence activities.
2. **Verifying claims made by those in power, to check the facts communicated by those in power.** Such claims may also be related to information influence and the techniques used. For example, claims may be linked to shared narratives in the field of information influence, or claims may be based on information from websites clearly intended to divide and polarise. Remember to distinguish between facts and opinions. The purpose of countering information influence is not to hinder freedom of expression but to contribute to a healthy climate of debate.

In summary, both branches of fact-checking involve scrutinizing what has been published as well as evaluating sources.

Verification system

First Draft formalised a system of verification that works broadly regardless of what is being verified, be it an image, content or an account:

- **Origin:** Is what you are about to verify actually the original image or content or account?
- **Source**: Who created the image, content or account?
- **Time:** When was the image, content or account created?
- **Place:** Where was the image, content or account created?
- **Motive:** Why was the image, content or account created?

There are numerous tools for, e.g., verifying images and social media searches. Many tools are free and relatively easy to use. Moreover, existing tools are constantly being developed and new ones are often added. The best way to learn is to try new things and cultivate curiosity. Many tools have excellent instructions that are easy to find when searching. There is no right answer or "correct way".

> **Verifying images, content or accounts, for example, is often detective work, where you use several different tools to find clues to put together.**

If a phone number, email address or other contact details emerge during your verification, the usual procedure under IFCN principles is to call, email or write a message to the disseminator to ask where the information came from, why it was published or shared, and so on. To verify pure facts, general journalistic principles of source evaluation apply — for example, try to find at least two

independent sources which are deemed authentic or credible. It has also become apparent in recent years that journalists and media outlets must be extra careful in verifying material and sources during sudden and/or dramatic news events. Such events often cause a lot of information to spread quickly, as newsrooms seek to be the first to report on what has happened.

Fact-checking when publishing on information influence

Fact-checking is not based on any journalistic or ethical principles that differ from those of traditional journalism. However, before any journalistic publication about information interference, e.g., a survey of information influence activities in the media outlet's circulation area, it is important to assess whether publication might encourage the spread of what the media organisation actually seeks to stop. The problem might be made bigger than it really is. At the same time, it is good not to wait too long. Once disinformation has gained momentum, e.g., on social media, it is difficult to slow its spread. Exactly where to draw the line varies from case to case, however, and each newsroom must try to determine where the line is for their circulation area. Content to be verified should also have some relevance to the audience, and it should matter whether the content is accurate or not.

> **One potential pitfall of fact-checking is the risk of shifting focus from what is really important to insignificant details.**

The importance of transparency

It is important to consider how you use images for publication. When fact-checking organisations around the world publish their reviews, they often publish the manipulated/incorrect image alongside the original. It is clearly stated which image is which. Under the standard used by the International Fact Checking Network (IFCN), a publication should also make clear how verification was carried out. The publication should account for all stages and sources of the verification process. If necessary, an expert should be interviewed to interpret the findings. Describing the publishing process is central to fact-checking and is also educational. The audience learns how to check material on the internet, and may begin to do so themselves.

Reflect on your choices and trade-offs

As a journalist, you should understand how your choices of news, angles, images and headlines matter, especially on social media, and that what you publish can stay online for a very long time. At the same time, of course, it's impossible to predict everything that might happen with, e.g., an article, and for journalists and media outlets a news item's relevance to the public is the most important factor in most cases

> **Your articles may be used for a completely different purpose than originally intended. Here, you as a journalist and your media outlet have an extra responsibility towards interview subjects and others involved in the content.**

The increasing prevalence of paywalls also means that the audience in some cases lacks access to all the necessary information for an accurate understanding of the content. Brainstorm this together in the newsrooms when you and your colleagues write headlines and posts for social media.

Moderating social media

Moderating a newsroom's social media comments section has become a common journalistic task. Bots and automated accounts may appear in the comments section, which you can read more about in this guide. When it comes to moderation, many newsrooms indicate that clear rules for comments are helpful. They can be a support for moderators when justifying why some posts are hidden or deleted, or even when accounts are blocked. Rules may include, for example, that commenters should stay on topic and that ad hominem attacks are prohibited.

Addressing threats and hostility directed at journalists

Information influence can be seen as a tactic to control which information is disseminated. Another way to do this is by subjecting journalists to hostility or even threats of physical violence. The Swedish Civil Contingencies Agency (MSB) has reported on this, in their report *Mediebranschen 2016 — hot, risker och sårbarheter* among others. The report states that the MSB assesses the risk that staff at media outlets in Sweden are physically or mentally injured as high. The MSB also describes how hostility and threats are now a daily aspect of the work of many journalists. This is also confirmed by the study *Journalisters utsatthet 2019*, by JMG at the University of Gothenburg, and by the Swedish Media Publishers' Association's *Hot mot kvinnliga opinionsbildare* from 2017. Beyond their effects for individuals, hostility and threats against journalists also impact the democratic system in several ways. For one thing, it becomes more difficult to recruit and retain journalists, and journalists may be reluctant to write about certain topics that they know in advance will generate hateful and offensive comments. In 2020, the Fojo Media Institute published the anthology *Det nya normala — ett hot mot demokratin*, with testimonials from Swedish journalists about hostility and threats in their day-to-day lives. Several international organisations, including UNESCO and the European Centre for Press and Media Freedom, are also working on these issues.

Support from Demokratijouren

Since 2017, the Media Institute Fojo has been commissioned by the Ministry of Culture to work on these issues. This work is carried out through the Demokratijouren project, which has more information on the subject. Fojo's Demokratijouren website provides basic preparedness advice for freelancers and newsrooms, information on the special support for journalists developed by various public bodies and authorities, and tips on current statistics, research and expertise regarding hostility and threats against Swedish journalists.

In an emergency, contact the police and your manager or employer.

Swedish work-environment legislation requires all businesses with at least one employee to have procedures in place to deal with a threat to an employee. This is part of systematic work-environment management. Whether you're a freelancer, an employee or a manager, Demokratijouren provides information on how to establish procedures to be prepared before threats arise. There is also advice on how to protect yourself from hostility and threats as well as what to do if you are targeted. Demokratijouren's ten tips for dealing with hostility and threats at work.

Demokratijouren's ten tips for dealing with hostility and threats at work

1. Think ahead. Conduct a risk analysis before, during and after publishing material that you suspect may attract hostility and threats.
2. Appoint a support person at or outside work. Decide in advance whom you will contact if and when you experience hostility and threats.
3. Draft an action plan. As a manager, employee or freelancer, decide in advance what to do and whom to contact during crises.
4. Stand up against hostility. Make it clear that it is unacceptable. Write an editorial policy against hostility and offensive comments.
5. Routinise support. Analyse daily any published content that may attract hostility or threats. Monitor and recognise when a reporter's well-being needs extra attention. Appoint someone to make it their job.
6. Avoid working alone. If working alone puts you in immediate danger, stop immediately. Check with your employer regarding routines for working alone. Find ways to work together, even if you are a freelancer or part of a small newsroom.
7. Let someone else handle the emails. When a tidal wave of digital hostility arrives, let a colleague or manager delete hate-mail and threats. Report any threats to the police and file the rest.
8. Don't Google yourself — ask someone else to check what is being written about you online.
9. Express solidarity with colleagues. Extend a helping hand to journalists subjected to hostility and threats. Offer backup and support.
10. Share your experinces about being victimised, provided that you are willing, ready and able. There is plenty of support and caring available. You are not alone.

For points 1, 3 and 4, templates are available at the Demokratijouren pages on the Fojo website.

Considerations for journalists faced with information influence activities

- Does your workplace have a plan of action if it is subject to attempted information influence activities? Can you learn from others, such as communication professionals in public administration?
- Does your workplace have an action plan for hostility and threats directed against employees? What resources are available, such as Fojo's Demokratijouren project?
- Many observers consider information influence activities a threat to democracy. How can the media better cover this development and describe to the public what is occurring?
- The relatively new journalistic genre of fact-checking, i.e., checking whether publications or statements are false, hardly exists in Sweden, unlike most of the Western world. What are the consequences for Swedish audiences?
- Was there an instance where you should have handled publication of certain material differently, e.g., in terms of headline or image? This may involve, e.g., showing consideration for interview subjects whose words were used in unrelated contexts, such as in information influence activities.

Glossary

Artificial Intelligence, AI

AI is the capability of a machine to display human-like traits, such as reasoning, learning, planning and creativity. AI enables technological systems to perceive their environment, manage what they perceive and solve problems, in order to achieve a specific goal (e.g., interpreting an image, summarising a text or composing a melody).

Bandwagon effect

A psychological phenomenon where people do something primarily because others are doing it. People who feel they belong to the majority are more likely to share their opinions and show their behaviours, so ideas and trends increase the more they are adopted.

Bot

A computer program that performs automated, repetitive tasks.

Disinformation

Deliberately false or manipulated information disseminated for the purpose of misleading people into opinions or behaviours that somehow serve the creator of that information.

Dark ads

An ad or post with tailored content created through psychographic profiling shown only to select members of a target demographic to influence their opinions or behaviours.

Eco-chamber or filter bubble

A natural grouping, online or offline, where people communicate primarily with others who share the same views and opinions.

Fake media

Counterfeit news sites designed to mimic genuine news sites.

Hacking

Exploiting weaknesses to breach security defences and gain unauthorized access to a computer or network.

Meme

A unit of transmitting cultural ideas, symbols, or practices that spreads from person to person; a cultural analogue to the gene, as memes self-replicate, mutate, and respond to selective pressures. Coined by Richard Dawkins in 1976. Memes can be images, phrases, concepts, or behaviours, often with humorous content, which are primarily spread over the Internet via social media.

Phishing

Fooling Internet users into providing their passwords or other sensitive information.

Potemkin village

False companies, research institutes, or think tanks created to give credibility to disinformation.

Shill

A promoter or spokesperson who gives the impression of being independent, but actually cooperates with or receives payment from someone else.

Sockpuppet

A false social media account used to sow discord in online debates anonymously, often arguing an extreme position. A common technique is to use sockpuppets to argue both sides of a debate.

Spiral of Silence

The psychological phenomenon when people remain silent if they feel their views are unpopular because they fear isolation or ridicule; when people who feel they belong to the minority don't share their opinions, the less likely it is that others who do share these opinions will voice them.

Strategic narrative

A compelling story that explains something about how we think and act, which is designed as a communicative action to support a specific purpose.

Strawman

The rhetorical tactic of misrepresenting an opponent's arguments to make it easier to refute them — a logical fallacy.

Symbolic act

An act performed primarily to communicate a message, rather than to benefit from any other practical consequences of that action.

Whataboutism

A cheap rhetorical tactic of shifting criticism from one's self by drawing a false comparison with an unrelated issue.

Strawman

The rhetorical tactic of misrepresenting an opponent's arguments to make it easier to refute them — a logical fallacy.

Symbolic act

An act performed primarily to communicate a message, rather than to benefit from any other practical consequences of that action.

Whataboutism

A cheap rhetorical tactic of shifting criticism from one's self by drawing a false comparison with an unrelated issue.

IN COLLABORATION WITH

Fojo
Linnaeus University

Swedish Psychological Defence Agency
Våxnäsgatan 10
653 40 Karlstad
E-mail: registrator@mpf.se
Switchboard: +46 10 - 183 70 00