Myndigheten för samhällsskydd och beredskap

Countering information influence activities

A handbook for communications officers

Countering information influence activities

A handbook for communications officers

Countering information influence activities
– A handbook for communications officers

This publication is also available in Swedish
Att möta informationspåverkan – Handbok för kommunikatörer
Order No: MSB1261 - Revised December 2018 ISBN: 978-91-7383-865-8

Swedish Civil Contingencies Agency (MSB)

Produktion: Advant

Publication number: MSB1260 - revised December 2018
ISBN: 978-91-7383-864-1

Innehåll

Foreword 5

Introduction 7

What is the communications officer's role? 8

Our approach 9

PART I. Becoming aware of information influence activities 11

What are information influence activities? 11

How are society's vulnerabilities exploited in information influence activities? 13

How are information influence activities different from other communication? 15

PART II. Identifying information influence 17

What is the purpose of the information influence activities? 17

Strategic narratives 17

Target groups 18

What techniques are used in the information influence activities? 18

Social and cognitive hacking 20

Misleading identities 21

Technical manipulation 23

Disinformation 25

Maligning rhetoric 26

Symbolic acts 27

How can influence techniques be combined? 28

PART III. Countering information influence activities 31

How can I prepare my organisation? 32

Raise awareness 32

Build trust through strategic communication 32

Know the organisation's risks and vulnerabilities 34

How do I choose the appropriate response? 35

Assess, inform, advocate, or defend? 35

Formulate a fact-based response 38

Special considerations for social media 40

How do I make use of lessons learned? 42

Strategic considerations 44

Glossary 45

More information 46

Foreword

The often-troubled state of the world today gives rise to the need to increase knowledge about how authorities can identify, understand, and counter information influence activities. Influence campaigns have become increasingly sophisticated and can be used both in peacetime and in war and can affect Swedish authorities' roles and responsibilities.

Information influence can exploit society's vulnerabilities and challenge how our society functions, including our fundamental values such as democracy, the rule of law and human rights, and ultimately life and health. At the same time, it is fundamental in the work of countering information influence activities to safeguard free debate, freedom of speech, and democratic discourse.

Our Government has decided that authorities must be able to identify and counter information influence campaigns and neutralise propaganda campaigns. The Swedish Civil Contingencies Agency (MSB) has therefore been working actively since 2014 to identify, understand, and counter information influence activities.

An important part of this work is increasing public awareness of information influence by disseminating knowledge.

In our work to increase knowledge about information influence, authorities responsible for monitoring such matters as well as others have expressed interest in a handbook covering the principles and methods for identifying, understanding, and countering information influence activities. MSB has therefore prepared this handbook in cooperation with researchers from Lund University. The handbook is mainly written for public sector communications officers. It should be viewed as an aid for situations in which an organisation is at risk of being subjected to information influence activities or suspects that it already has been.

MSB would like to express its great appreciation to the Department of Strategic Communication at Lund University, the research of which forms the basis of the handbook, as well as the referral bodies that, with their wise comments, contributed to developing the handbook. MSB would also like to thank the authorities and organisations that contributed to making the handbook better and more useful for their own organisation.

Dan Eliasson

Director-General

Introduction

Introduction

The changing state of world affairs and an increasingly complex security situation form the backdrop to the preparation of this handbook. The illegal annexation of Crimea and the conflict in Ukraine have shown how security threats today can take on a different character. In this kind of conflict, non-military means are primary tools.

Influence campaign is the term used to describe this new type of security threat. In influence campaigns, foreign powers exploit a society's vulnerabilities to achieve their goals without the need for military force.

Influence campaigns are therefore a phenomenon that we need to defend ourselves against in order to safeguard the goals of Sweden's security and to maintain the life and health of our population, the functioning of our society, and our ability to preserve fundamental values such as democracy, the rule of law, and human rights and freedoms.

MSB defines influence campaigns as coordinated activities by foreign powers, including the use of misleading or inaccurate information or other means, to influence political or other public Swedish decision-makers, the opinions of all or part of the Swedish population, and decisions or opinions in another country that might negatively affect Sweden's sovereignty, the goals of Sweden's security efforts, or other Swedish interests.

An influence campaign consists of several influence activities, of which information influence is one. This handbook helps you, as a communications officer, to become aware of what information influence is so that you will be able to identify and counter this kind of security threat.

The use of information to influence others is nothing new. In areas such as public relations and advertising, information is used to influence people's decisions to buy a certain product or to support a certain political candidate. As public, we expect such communication to follow certain rules such as transparency, that it is based on accurate information, and that it is all presented in a way that makes it possible for the public to make well-informed choices.

However, far from all influence activities play by these rules. Information can be used covertly and deceptively by foreign powers to undermine democratic processes, control public discourse, and influence decision-making in order to increase foreign influence. These are called information influence activities. From a global perspective, there are a number of recent examples where this particular kind of influence has been identified, such as the presidential elections in the United States in 2016 and in France in 2017. Information influence activities have hostile intent, but are not defined as acts of war, although they are sometimes referred to as information warfare in a grey zone between war and peace. They are to be considered hostile because they risk undermining public confidence in critical societal institutions, isolating vulnerable groups in society, and contributing to social and political polarisation.

Our society is built on trust, including both public confidence in the institutions of society and the trust between people and groups in society. Confidence and trust are a prerequisite for democracy to work well. Information influence undermines these values by sowing the seeds of mistrust and fanning the flames of conflict in society. When foreign powers use information influence against a population, it can be a threat to national security. The ability to maintain confidence and to counter information influence activities with trustworthy communication is absolutely crucial for a resistant society.

What is the communications officer's role?

As a communications officer, you can play a key role in preventing, identifying, and countering information influence activities. You contribute to your organisation keeping its promises and safeguarding public confidence. You communicate with your target groups, help them when they have questions, and give them information that is vital to society. As a communications officer, you know what your target groups think is important and what is on their agenda.

Even if it seems improbable, your organisation might one day be the target of information influence activities. You might discover that incorrect information is spread about your organisation, that false versions of your website appear, or that your accounts on social media have been hijacked. Information influence activities can also be directed straight at the organisation's target groups by them being subject to so-called cyber bullying, trolling, or misleading information. The goal might be to undermine confidence in your organisation, to present incorrect information in important discussions in your field of activity, or to increase tensions between your target groups.

In all cases, as a communications officer you have the opportunity to play an important role in the work to strengthen and support a constructive democratic debate.

WHY COMMUNICATIONS OFFICERS?

- You build bridges between organisations and the public.
- You already work with crisis communication, which can be a relevant tool for countering information influence activities.
- You might be among the first to discover signs of information influence activities.

As a communications officer, you already have tools needed to counter information influence activities. This handbook gives you additional knowledge that can support you in this work. You will learn about the techniques that can be used against you and how to recognise early warning signs that something is in the making. You will get advice on how to prepare your organisation to quickly and effectively counter the information influence activities and guidance on how to make the right decisions about countermeasures based on the specific situation and your mandate as a communications officer.

Our approach

The purpose of this handbook is to help you as a communications officer to develop your knowledge about and ability to identify and counter information influence activities.

The goal is to raise awareness and knowledge about information influence activities. The handbook is intended to make it easier to identify common methods used in information influence activities that your organisation might be subjected to, and to provide a toolbox of communicative actions that can be used to design an appropriate response. This handbook does not provide all the answers as to what you should do. All organisations are different and have different target groups and face different types of challenges, and they need to take these factors into account in their response.

PART I: BECOMING AWARE OF INFORMATION INFLUENCE ACTIVITIES

What are information influence activities?

How do information influence activities exploit society's vulnerabilities?

How are information influence activities different from other communication?

PART II: IDENTIFYING INFORMATION INFLUENCE ACTIVITIES

What is the purpose of the information influence activities?

What techniques are used in the information influence activities?

How can these techniques be combined?

PART III: COUNTERING INFORMATION INFLUENCE ACTIVITIES

How can I prepare my organisation?

How do I choose the appropriate response?

How do I make use of lessons learned?

PART I.
Becoming aware of information influence

What are information influence activities?
How do information influence activities exploit society's vulnerabilities?
How are information influence activities different from other communication?

PART I. Becoming aware of information influence activities

This section describes how the information influence activities exploit vulnerabilities in societies.The section also presents a tool for assessing suspicious activity and identifying cases of information influence.

What are information influence activities?

Free debate, differences of opinion, and attempts to convince people are important parts of a well-functioning democratic society. But what happens when someone fabricates evidence, uses false experts, or argues in a deliberately misleading way? Such communication is detrimental to society and is a problem for the democratic process. An appropriate response is based on facts, source criticism, and the principles of freedom of speech in order to protect our democratic society.

In most democracies, there is free and lively political debate in which private citizens, journalists, academics, and representatives from civil society see it as their duty to point out clearly incorrect and misleading information in addition to the important scrutiny of power. State actors can support this work by, for example, providing financial support and contributing to correcting inaccuracies linked to their own activities. This system has long served democracies well, at least in theory. However, today's debate about false news suggests that the system is characterised by vulnerabilities, which foreign powers exploit through information influence activities.

Information influence activities are potentially harmful communications deliberately or indeliberately enacted by foreign powers or their agents. Attempts to create distrust between citizens and between citizens and the state constitute deliberate interference by foreign powers in national affairs. Information influence activities are used to support the agenda of foreign powers, and they are designed to exploit perceived vulnerabilities in society. By studying a society and its conflicts, controversies, and challenges, information influence activities are targeted at these vulnerabilities in order to increase the fragmentation of the society.

Information influence activities can be carried out as individual activities or as part of a broader influence campaign. In the latter case, a wide range of techniques are used both from within and outside the field of communications. In addition to communicative tools, everything from diplomatic and economic sanctions to demonstrations of military force are used to influence a society.

THE ANATOMY OF INFLUENCE CAMPAIGNS

The use of influence techniques

Public relations, marketing, diplomacy, op-eds, and lobbying are examples of acceptable ways of influencing people's views and behaviours. Information influence activities mimic these but might also include mudslinging in different forms and might use the techniques to mislead, such as deliberately lying or fabricating information.

Disrupting public debate

Foreign powers use information influence activities to influence areas and debates when they benefit from such activities. This can be done both directly and indirectly through everything from open propaganda to covert funding of civil society groups that do the bidding of foreign powers. By interfering with public debate, our view of public opinion or streams of thought can change and thus influence decision-making.

Acting out of self-interest

The purpose of the information influence activities is to achieve specific objectives that benefit a foreign power. The objective can be anything from destabilising a society politically, preventing specific decisions from being made, or creating polarisation between groups in society.

Exploiting vulnerabilities

All societies have their challenges. Sometimes these consist of tensions between different groups, inequality, corruption, security, or other central issues in society. Within information influence activities, these vulnerabilities are systematically identified and exploited.

Information influence activities are characterised by a certain ambiguity. This means that it is sometimes difficult to determine what is a genuine element of public debate. Political debates can be sensitive, uncomfortable, and sometimes even dirty.

This is a natural part of the democratic process that is based on openness and the possibility of debate between people with different opinions. But such a discussion is difficult to conduct in a productive and constructive way if foreign powers introduce misleading information in order to disrupt and control the conversation.

It is important to remember that a sender does not automatically sympathise with foreign powers simply because he or she expresses similar views. It is important to emphasise that in information influence activities deceptive practices are used systematically in order to undermine democracy. Therefore, a fundamental principle in countering information influence activities is to safeguard free debate, freedom of expression, and the democratic dialogue – this cannot be emphasised enough – even if it complicates the task.

How are society's vulnerabilities exploited in information influence activities?

Let us assume that our opinions are formed as a result of a rational process that begins with something happening or new information coming to light. Witnesses, researchers, officials, and other individuals with credibility in an area interpret or explain the situation in a broader context. The media pick up the descriptions and spread them through their channels. This information will thus reach different groups in society, both online and offline, including you. Of course, opinion formation does not quite work like this in practice, but this is broadly how the process of opinion formation in a democratic society can be understood.

This process is based on a few basic principles. First of all, it depends on the event or information being correct and based on facts. It also assumes that the claim is verified by credible sources in the form of individuals whose reputation will be undermined if they lie. It assumes that the media that pick up the story are balanced in their coverage, that they double-check facts and sources, and that they strive to serve the public interest. We also expect discussions in various groups of society to take differing voices and opinions into account and a constructive debate to be conducted before drawing any conclusions.

Information influence activities exploit situations in which opinion forming deviates from the process described above. Through opportunistic, creative, and technologically advanced methods, foreign powers can direct their influence techniques at vulnerabilities of the opinion-forming process in order to compromise the flow of information. Foreign powers identify vulnerabilities in how critical information travels through the media landscape and in how our brains process information.

Facts can be falsified or manipulated. False experts can be called in, and witnesses can be coerced. News services can be run as one-sided propaganda channels, and the digital public discourse can be conducted between automated bots that create the false appearance of a lively public debate. When these activities are carried out deliberately, sometimes in the form of coordinated campaigns with the aim of undermining democratic processes, we cannot always rely on a self-adjusting system. As a communications officer, you can play an important role here.

Opinion formation

NEW INFORMATION

New information may reach us through an event, a scientific discovery, a media revelation, or a political decision.

EXPERTS, OFFICIALS AND SOURCES

New information is observed and documented by witnesses, experts, and/or officials who explain or interpret the information.

MEDIA AND CULTURE

The information reaches the public through media and other forms of cultural expression such as newspapers, television, radio, blogs, or social media.

PUBLIC SPHERE

The information reaches the public sphere and is processed through discussion and dialogue within different groups in society, both face to face and on social media.

THE INDIVIDUAL

In this way, the information reaches you as an individual through the social structures you are a part of and the channels you consume.

VULNERABILITIES IN THE MEDIA SYSTEM

Our modern media system has several vulnerabilities, especially in relation to the changing technology landscape, new journalistic business models, and the growing number of alternative online news sources. Everything from forged letters and manipulated images to clickbait, algorithms, and bots on social media make the media system vulnerable to those who want to use it for their own gain, whether it is driven by economic or political motives, or simply to see if it is possible.

VULNERABILITIES IN OPINION FORMATION

Opinion formation has always been vulnerable based, for example, on the idea of social proof (i.e. what someone claims to have experienced themself). In today's information environment, where fake accounts on social media and trolls distort the debate online, it is easier than ever to fabricate social evidence and to provoke and incite anger and outrage. This helps to polarise political debate and is therefore a vulnerability in public opinion formation.

COGNITIVE VULNERABILITIES

Some vulnerabilities arise as a result of how our brains work. We are simply not made to handle all of the information we are exposed to in today's society. For example, through so-called psychographic methods, personal information about us online can be used to understand how we function even better than we understand ourselves. According to some estimates, there are up to 800 data points for every individual on social media that can be used to predict opinions and behaviours. In information influence activities, our thought patterns are exploited together with information about us to influence our perceptions, behaviours, and decision-making.

How are information influence activities different from other communication?

It is not the role of the communications officer to investigate whether a foreign power is responsible for specific communication activities. You are expected to act in cases when you suspect that information influence is used in debates linked to your operating area or in order to undermine the integrity of public debate and the security of society. It is important to understand the role of your own organisations in a wider context and in a social perspective.

To identify cases of information influence, you need to assess the extent to which communication is misleading, intentional, and designed to disrupt. By weighing these factors together when assessing a suspected case, you have the opportunity to make an informed decision on how to formulate your response. All indications will not necessarily be seen simultaneously, but the more indications you identify, the higher the likelihood that information influence activities are being conducted.

MISLEADING

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

INTENTIONAL

Reliable communication aims to contribute to and strengthen constructive debate, although the content or arguments might be controversial in themselves. However, information influence activities have the intention of undermining constructive dialogue and open debate.

DISRUPTIVE

Reliable communication is a natural part of our society and strengthens our democracy, even it sometimes causes friction. Information influence activities disrupt and weaken the functioning of our society and democratic dialogue.

It is no coincidence that techniques used in information influence activities often overlap those used in journalism, public diplomacy, lobbying, and public relations. Emulating these methods is a way of concealing information influence activities and making them appear to be reliable information. Illegal influences, such as threats, hacking, extortion, or bribery, fall outside this discussion and should be reported to the police.

PART II.
Identifying information influence activities

What is the purpose of the information influence activities?
What techniques are used in the information influence activities?
How can different techniques be combined?

PART II. Identifying information influence

A prerequisite for countering information influence activities is the ability to detect potential cases. This means that you need to know what to keep an eye out for. This section presents a detailed description of the techniques used to conduct information influence activities and helps you evaluate strategic narratives and techniques for adaptation to the target audience. It also provides an introduction to the most common techniques and shows how they can be combined into coordinated actions.

What is the purpose of the information influence activities?

To identify information influence activities, you first need to know about two overall strategies used in information influence activities, namely strategic narratives and targeting techniques. Knowledge of these can help you identify information influence activities and can contribute insights into the purpose of the influence activities.

Strategic narratives

Information influence activities usually include some kind of storytelling, and the portrayal of an event, issue, organisation, location, or group is usually formulated to fit into an existing narrative. For example, most people have heard of the space race between the United States and the Soviet Union during the Cold War. Most people have heard stories of how man landed on the moon; others have heard stories that everything is a lie. On video, we can see astronauts planting a flag on the moon; some take this as proof that the moon landing took place and others claim instead that it is faked. These are typical narratives that are used unconsciously to sort new information. When we hear new stories about space travel, we sort the information and evaluate it in relation to which of these versions we believe in. When such stories are designed and communicated for the purpose of achieving a particular goal, they are called strategic narratives.

For example, you can find things about some ethnic or religious groups that fit in with people's preconceived ideas about these groups, i.e. the existing narrative. The discussion can be influenced in three different ways – by highlighting parts of the existing narrative, by pushing away other narratives, or by making new connections to unrelated events in order to distract.

Identifying strategic narratives and the logic behind information influence activities is an important step in preparing and developing appropriate response strategies to counter information influence activities. Consider whether you can see strategic narratives used in any of the following three ways:

STRATEGIC NARRATIVES

Positive or constructive: "This is the truth!"
Tries to construct a coherent story about a particular issue that fits in, complements, or develops existing narratives.

Negative or disruptive: "This is a lie!"
Aims to prevent the emergence of coherent narratives or to undermine existing narratives on an issue.

Oblique: "Look over here!"
Draws attention away from a particular issue or argument by distracting the discussion. For example, humour, memes, or conspiracy theories are often used in this respect.

Target groups

Analysing strategic narratives is one of several approaches to understanding the logic behind suspected cases of information influence activities. Another approach is to analyse whom these strategic narratives are talking to, i.e. who the intended target group is. Are narratives targeted at the whole population or more specifically at individual groups or individuals? Are big data used to design targeted actions against people with similar personality traits and opinions? Is targeting used to exploit vulnerabilities or behavioural patterns associated with a specific group or individual? If you know to whom a story is aimed at, it will be easier to understand the underlying purpose and how the information influence is meant to work in the specific case.

TARGET GROUPS

General societal level: mass audiences
Information influence activities are directed at broad groups in society or society as a whole by using large, common narratives.

Sociodemographic targeting: specific groups
Specific target groups are identified based on demographic factors such as age, income, education, or ethnicity. This way you can create messages tailored to appeal to the group's members.

Psychographic targeting: individuals
Data on individuals are used to identify specific personality traits such as political preferences or behavioural patterns that can form the basis for individually adapted communication.

Target group analysis can reveal the intent of information influence activities. If you analyse the strategic narratives and communication techniques used, you can get an idea of who the intended recipient is, thus creating an understanding of the purpose and objective of the information influence activities. This will in turn help you to decide which countermeasures are most appropriate.

What techniques are used in the information influence activities?

Within information influence activities, a number of techniques are used to influence people's decisions. The techniques are under constant development, and the common techniques can be divided into six overall groups. Within each group, the techniques are characterised by similar principles. By understanding what these technologies look like and how they work, you can more easily recognise and identify information influence activities.

In most cases, the techniques are neutral. The same technique can be used as a natural part of the democratic dialogue (where it is applied in an open and accepted manner) or as a technique in information influence activities (where it is used to mislead the public). Therefore, the presence of a particular technique in your area is not necessarily a sure sign of information influence activities.

Instead, you should proceed from your assessment of the extent to which the activity is intentionally misleading in order to harm society and use your analysis of strategic narratives and targeting to answer the following questions:

- How strong are the indications of deceptive and disruptive purposes?
- What do the strategic narratives and the intended target group say about the purpose of the communication?
- If the use of any specific technique occurs, is it used in a way that could be harmful to the public or to society?

Information influence techniques

SOCIAL AND COGNITIVE HACKING (PAGE 20)
- Dark ads
- Bandwagon effects
- Spiral of silence
- Echo chambers and filter bubbles

DECEPTIVE IDENTITIES (PAGE 21)
- Shilling
- Impersonators and imposters
- Forgeries
- Potemkin villages
- Fake media

TECHNICAL MANIPULATION (PAGE 23)
- Bots
- Sockpuppets
- Deepfakes
- Phishing

DISINFORMATION (PAGE 25)
- Fabrication
- Manipulation
- Misappropriation
- Satire and parody

MALIGNING RHETORIC (PAGE 26)
- Ad hominem
- Whataboutism
- Gish-gallop
- Strawman
- Hijacking

SYMBOLIC ACTION (PAGE 27)
- Leaks
- Hacking
- Public demonstrations

Social and cognitive hacking

Social and cognitive hacking exploits our social relationships and thought processes. It is similar to hacking of computer systems in the sense that a hostile actor is trying to deceive or "hack" a process by exploiting its vulnerabilities. For example, we usually prefer to adapt to what people like us think and do, and we sometimes have difficulty thinking rationally when we are exposed to emotionally charged content. These predictable patterns of behaviour can be exploited by hostile actors who deliberately target sore points, for example, on sensitive societal issues, in order to achieve their purpose

DARK ADS

Messages that are tailored to an individual's psychographic profile. Data from social media, for example, can create databases of individuals with specific beliefs, interests, or personality traits. Ads that can only be viewed by specific individuals might contain messages that appeal to their specific preferences or opinions.

BANDWAGON EFFECT

People who feel they are part of a majority are more likely to share their opinion. Bots and trolls can be used to provide more likes, comments, or shares on social media in order to give the impression that some opinions are more popular than they actually are. This creates social acceptance for a message or an opinion, which appeals to our cognitive need for social conformity.

SPIRAL OF SILENCE

People who feel they are in a minority are less likely to share their views. In contrast to the bandwagon effect, the impression that you are in a minority can make you not want or dare to speak. This appeals to our fear of being excluded or pointed out as deviant.

ECHO CHAMBERS AND FILTER BUBBLES

Organic groupings within which people mainly communicate with others who share the same views and beliefs. Echo chambers and filter bubbles can occur both online and offline. People with similar views might read the same newspapers or mainly hang out with like-minded people. They are therefore rarely exposed to ideologically different opinions. On the Internet, this can be used to spread targeted information to specific groups.

Misleading identities

When we assess information, we often look at the source. Who is communicating with me and why? What do they know about the issue? Who do they say they are? Actors can emulate credible sources of information such as people, organisations, or platforms and use deceptive identities to exploit the messenger's capital of trust.

SHILLING

A shill is a person who gives the impression of being independent, but in fact works with or receives payment from someone else. Shills are sometimes used to write positive product reviews in online shops and to lend credibility to a person or a message. This can be equated with a purchased audience that guarantees applause after a performance. In information influence activities, shills might be a group of Internet trolls that are paid to write comments.

IMPERSONATORS AND IMPOSTORS

Impersonators pretend that they are someone other than they really are, meaning they take on the identity of someone else. This might involve impostors claiming to have expert knowledge or qualifications they actually lack, for example, by claiming to be a doctor or a lawyer without having completed the required training.

FORGERIES

Fabricating and forging information is an effective way to make disinformation look like authentic information. False letterheads, stamps, or signatures might be used to make pure forgeries look genuine.

POTEMKIN VILLAGES

Actors with sufficient resources can go one step further and create false and deceptive institutions and networks. Fake companies, research institutes, and think tanks are examples of what are called Potemkin villages that might be created and used to lend authenticity to disinformation.

FAKE MEDIA

Disinformation might also be spread through forged news sites that mimic genuine ones. On the Internet, for example, you can create a fake website that is almost identical to a real website, but with different content.

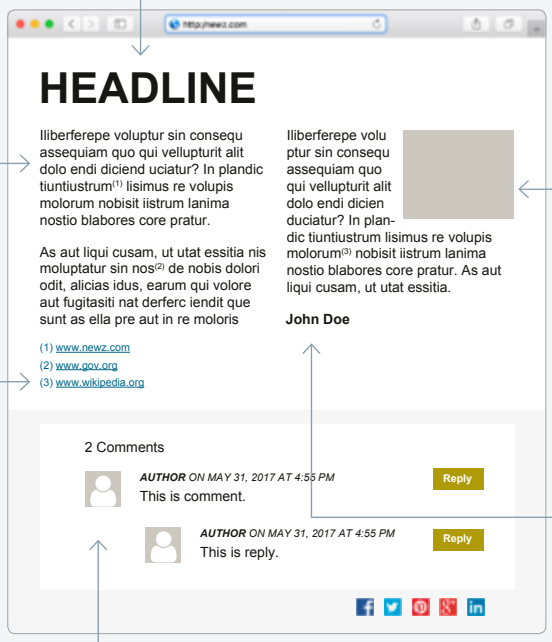
Source criticism online

HEADING
Headings try to elicit interest and response from the reader. Always read more than just the heading and make sure that the heading matches the rest of the article's or page's content.

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

CONTENT
Do an assessment of the content of the text. Is it informative or argumentative and is it based on facts, emotions, or opinions? Always read the entire text before sharing or spreading it.

IMAGES
Images are not always a reflection of reality. Images can be easily manipulated by elements being deleted, edited, or added. It is also not certain that the image has a real connection to the content. Through an image search, you can find out if the image was previously used in any other context.



SOURCES
If the text refers to other sources, make sure to check them and trace the origin of the information. Do an assessment of whether the sources are used correctly in the text.

AUTHOR
Be careful of texts without authors. If there is an author, think about who it is and why that person wrote the text.

COMMENTS
Comments on websites and social media are usually made by ordinary people expressing their views.
However, there might also be troll accounts and bots in the comment fields. Pay attention to who comments.

ENGAGEMENT
A text being liked or shared a lot does not mean that the content is accurate. Be wary of sharing something solely based on the attention it received from others.

Technical manipulation

Information influence activities often take advantage of modern technology to achieve their effects. With advanced technical skills, individuals can manipulate the flow of information on the Internet through automated accounts and algorithms or a combination of human and technical manipulation. Note that technical manipulation often uses new tools to perform traditional influence techniques, such as creating deceptive identities online or creating and spreading disinformation. Such areas are developing far faster than our ability to analyse potential consequences and areas of use. In the near term, problems caused by deepfakes, machine and deep learning, and artificial intelligence (AI) are well-known, and we can expect this type of technology to be used in the future to a greater extent.

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 service platform. In information influence activities, bots can be used to reinforce selected messages online, spam forums and comment fields, like or share posts on social media, or carry out cyber attacks.

SOCKPUPPETS

False accounts typically belong to an individual who does not reveal his or her true identity or intentions. These false identities are used to join groups and participate in online debates. Two or more sockpuppets can be used simultaneously to simulate both sides of a debate.

DEEPFAKES

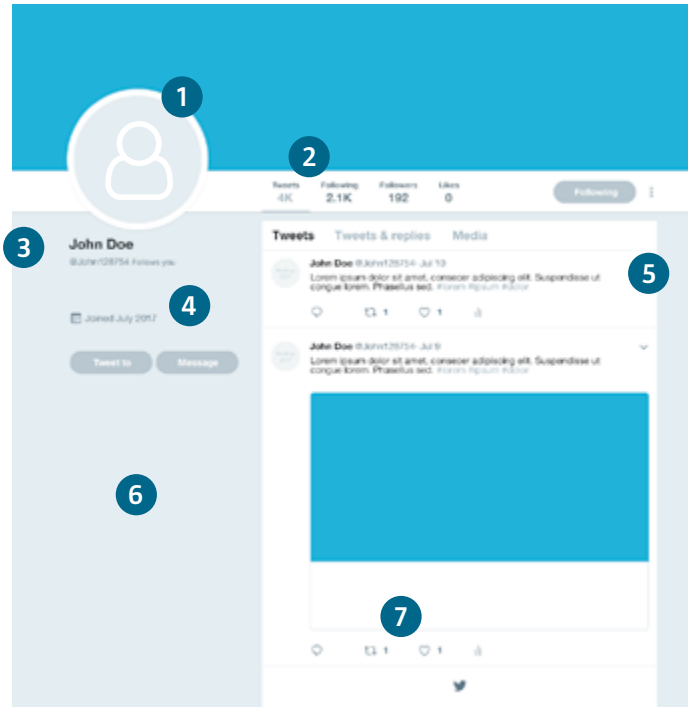
Modern learning algorithms can be used to manipulate audio and video in very advanced ways. It is, for example, possible to produce false but very credible videos in which politicians deliver imaginary speeches. You can also change the faces of people in existing videos or digitally modify or reconstruct a person's voice.

PHISHING

Phishing is a technique that tricks users into providing passwords or other sensitive information. Phishing also includes automated spamming via email messages that appear to have been sent from a known sender but actually belong to a scammer who is looking for personal information. Spear phishing is a sophisticated type of phishing to access information on secure computer systems.

How to detect a bot

Bots are effective tools to conduct influence activities on social media. But they are also relatively easy to expose. These seven steps will help you identify bots on social media. Bots occur in different forms and can look very different. Impersonator bots try to emulate real users and can be difficult to detect. Spam bots, on the other hand, focus on spreading information quickly and widely and are therefore easier to recognise.



1 PROFILE PICTURE

Bots either use a stolen profile picture or they do not have a profile picture at all. Conduct an image search to verify the authenticity of the profile picture.

2 ACTIVITY

Many bots are very active, sometimes with up to 50 posts a day. Be careful of accounts with a suspiciously high number of posts per day.

3 NAME

Most bots generate their user names automatically. If you discover accounts with user names that appear to be random, this might be a sign of a bot.

4 ACCOUNT CREATION DATE

Many bot accounts are created in direct connection with the bot being used and are therefore very new. Older accounts are sometimes used, but old posts are often deleted, resulting in a large gap between the creation date and the first post.

5 LANGUAGE

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

6 INFORMATION

Bot accounts often lack personal information or use fictional or forged information. Check the information provided.

7 INTERACTION

Check which posts and other users the account is interacting with. Bots are often coordinated and mutually reinforcing, while having few followers that are not bots.

Disinformation

Disinformation refers to inaccurate or manipulated information that is deliberately spread in order to mislead. This is a cornerstone of classic propaganda and forms the basis of contemporary discussions of so-called ”fake news”. Deliberately using disinformation to mislead is nothing new, but digital platforms have created new opportunities and changed the nature of disinformation. Incorrect information might occur in the form of manipulated text, images, video, or audio. These elements can be used to support false narratives, create confusion, or discredit credible information, individuals, or organisations.

FABRICATION

Incorrect information that is published in a way that makes the recipient believe that it is true. Fabricated e-mails from a politician could, for example, be produced and leaked to the press to undermine the credibility of the politician.

MANIPULATION

Information that is manipulated to communicate a misleading and incorrect message, such as adding, deleting, or modifying elements of text, images, video, or audio clips.

MISAPPROPRIATION

Presentation of the correct facts in an unrelated context to present a question, event, or person in a misleading manner. For example, images taken in other contexts can be used to amplify the narrative in a news article.

SATIRE AND PARODY

Satire and parody are normally harmless forms of entertainment. In information influence activities, however, humour can be used as a tool to spread misleading information and ridicule or criticise individuals, narratives, or opinions. Humour can also be used to legitimise controversial opinions.

Maligning rhetoric

Rhetoric is an accepted and natural element of democratic social debate, where everyone has the right to express their opinion. Maligning rhetoric is pursued for a different purpose. It might be about using public discourse in order to mislead or distract the audience. It might also involve strategies to deceive, mislead, and/or deter certain actors from participating in public debate.

An actor who often uses maligning rhetoric is a troll. Trolls are social media users who deliberately provoke others through their comments and actions online. Their activity contributes to increased polarisation, silences critical voices, and drowns out open debate. Trolls can be driven by personal motives or can work on behalf of someone else (also known as *hybrid trolls*).

AD HOMINEM

To attack, discredit, and ridicule the person behind an argument instead of criticising the argument itself. Ad hominem is often used for the purpose of silencing, preventing, and discouraging others from participating in the discussion.

WHATABOUTISM

To change the focus from an argument by highlighting a similar phenomenon that has not received as much attention, but which is not really relevant to the issue.

GISH-GALLOP

To overwhelm the opponent with a flood of arguments, facts, and sources, many of which are false or unrelated to the issue.

STRAWMAN

To impute to an opponent arguments and positions the opponent does not stand for, and then argue against these positions instead of the opponent's actual positions..

HIJACKING

To take over a debate and change its direction. This is particularly effective on social media in relation to hashtags and memes.

Symbolic acts

Actions speak louder than words. Sometimes the purpose of a document is primarily to communicate a message. This is called a symbolic act. Unlike ordinary actions, symbolic acts are motivated by communicative logic and strategic framing. They can be designed so that the message is obvious to everyone, such as acts of terrorism in which actors play on the universal fear of irrational violence. At other times they are more subtle, like when you use cultural symbols that are only relevant to a particular target group.

LEAKS

Leaks have a strong symbolic significance because they can reveal injustices and blackouts that are not otherwise known to the public. However, in information influence activities, information is often leaked out of context and used to systematically undermine the credibility of an actor and to distort the information environment. The leaked information might have been obtained through, for example, computer hacking or theft.

HACKING

Hacking involves acquiring unauthorised access to a computer or network and is in itself a crime. In information influence activities, hacking is sometimes a symbolic act in which the intrusion itself is secondary. The actual objective is to arouse suspicion that a system is exposed or not secure, which might undermine confidence in the system in question or in the organisation responsible for the system.

PUBLIC DEMONSTRATIONS

Demonstrations are symbolic acts used to express support for a particular political issue or position and are important elements of our democratic dialogue. In information influence activities, demonstrations might be orchestrated to give a false impression of support for a given issue at a grass roots level (so-called astroturfing).

How can influence techniques be combined?

To identify cases of information influence activities, you need to assess the strategic narratives, target groups, and techniques that are used. In the assessment, you should consider that several techniques are often combined to achieve a greater effect.

For example, a forged document can be widely spread using bots. The effect is amplified even more if the operation is coordinated with biased articles spread on fake news platforms, which are then commented on by a coordinated group using trolling techniques. Therefore, consider whether there is evidence of not only occasional, but also multiple coordinated activities directed at your organisation. On the next page, you will find some examples of what combinations of techniques might look like.

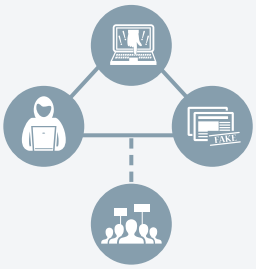
We have proposed a few different questions you can keep in mind when assessing communication and identifying the impact of information. What are the narratives and whom are they targeting? Is there evidence to support the claim that someone is trying to mislead or interfere with public discourse? Do you suspect direct interference from a foreign power or indirectly through their agents? Do you see signs of combinations of methods that suggest a coordinated action or campaign? If your assessment is the basis for suspecting information influence activities, you will find suggestions for countermeasures in the next part of the handbook (Part III: Countering information influence activities).

Combined techniques

The above techniques are rarely encountered individually, but are often combined to achieve greater effect. You should be wary of the combinations of techniques that you might be exposed to. There are many possible combinations, but some of the most common combinations are useful to know.

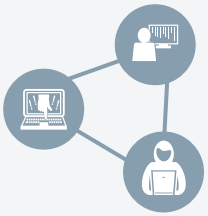
Polarisation

Polarisation combines social hacking, deceptive identities, and disinformation to stoke extreme positions on an issue. Trolls and bots are often used to reinforce extreme opinions.



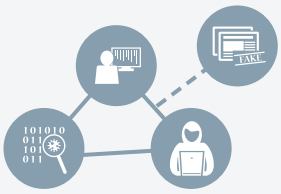
Laundering

Laundering combines deceptive identities, disinformation, technical manipulation, symbolic acts, and social and cognitive hacking to gradually distort and decontextualise information so that it becomes very difficult for the recipient to determine what is true or false



Provocation

Provocation exploits sensitive issues in society to agitate people and create anger and discord. The combination uses mainly social and cognitive hacking, deceptive identities, and maligning rhetoric.



Flooding

Flooding aims to overload an audience with information through spamming and trolling on social media or by spreading disinformation through media sources in order to crowd out reliable information.

PART III. Countering information influence activities

How can I prepare my organisation?
How do I choose the appropriate response?
How do I make use of lessons learned?

PART III. Countering information influence activities

This section discusses different methods for countering information influence activities. It describes how you can prepare your organisation, discusses various countermeasures, and provides suggestions on how your organisation's knowledge and experiences can be spread, thereby contributing to knowledge transfer across organisational boundaries.

PREPARE

Raise awareness
Build trust
Assess risks

ACT

Choose your response
Fact check
Use social media

LEARN

Describe
Reflect
Share

How can I prepare my organisation?

Preparation is essential. By preparing people and establishing functioning structures to counter information influence activities, it is possible to respond rapidly and effectively so as to mitigate the effects of such activities. The preparations consist of three main parts – raising awareness about information influence activities; developing messages, narratives, and an understanding of how your target groups and stakeholders are vulnerable to different types of information influence; and carrying out a risk and vulnerability analysis of your organisation in order to identify and prevent information influence activities.

Raise awareness

An important part of creating readiness to manage information influence activities involves raising awareness of the threats and vulnerabilities faced by society in general and your organisation in particular. At the societal level, the best defence is to create meeting places where, for example, leaders, journalists, representatives of social media platforms, researchers, communications officers, and citizens can exchange knowledge and lessons about countering information influence activities.

As a communications officer, there are also things you can do to build capacity within your organisation. Firstly, you can be an important contact point through your knowledge in the field. It is especially important that you conduct discussions with senior management and communicate internally with colleagues regarding questions related to the subject. Secondly, you should have an advisory role in relation to your managers and colleagues regarding what action should be taken in the event that your organisation is subjected to information influence activities. This includes identifying the need for and possibility of training. Thirdly, you should build networks consisting of professionals, even outside your organisation, based on mutual support and exchange of experiences. Fourthly, increased transparency and awareness of your organisation's activities can prevent the spread of false information.

Build trust through strategic communication

One of the objectives of information influence activities is to undermine people's confidence in the institutions of society. The effect can therefore be minimised by focusing on countermeasures that build trust in the organisation. This is a very important part of all strategies to counter information influence activities.

Preparing communications

Because it might take time to get messages approved in crisis situations, it is important to prepare generic messages ahead of time. These messages should be formulated based on the values of the organisation and in such a way that they can be easily adapted to specific events. In the same way that organisations use messages to talk about new initiatives or a new product, messages can also be used to create awareness of false stories or to refute them.

PREPARING MESSAGES

Sharing accurate information at the right time is made possible by solid preparatory work, where finished messages have been prepared and approved even before something happens. A good example is the London police, who sent their first tweet only seven minutes after the terror attack at Westminster in March 2017. The message contained accurate information about the on-going situation and was based on a communication template developed for similar situations that could be quickly adapted to the current sequence of events.

It is important to take into account the stories circulating about your organisation and what overall narratives are being pushed when a message is formulated. Narratives are linked to the perceptions of the target audience. Consider how individual messages contribute to the values and narratives your organisation wants to communicate, especially in relation to different target audiences. Messages that build confidence in your organisation play an important role in developing resilience to misleading and false information.

WHAT IS YOUR STORY?

Messages should be adapted to the overall narrative that you want to communicate.

A strong narrative comes from clear values and goals within your organisation.

Analysis and understanding of what factors contribute to the narratives that your organisation wants to convey create an understanding of the organisation's vulnerabilities.

Attacks are best met by maintaining the values that your organisation stands for.

Get to know your target audience

By first establishing your organisation's core values, messages, and desired narratives, you can then map out various vulnerabilities and which of your organisation's target groups and stakeholders are most vulnerable to information influence activities. These target groups and stakeholders are prioritised in cases where information influence activities are identified.

As a communications officer, you will in all likelihood have previous experience of target group analysis. You need to use a method to analyse which target groups are most vulnerable to information influence and why. As a communications officer, your job is to identify which parts of your organisation, its target groups, and its users might be subject to information influence activities and to consider what kinds of messages they might be susceptible to. Once you have done this, you can make suggestions about how to reach these target audiences with countermessages and preventive communication.

TARGET AUDIENCE ANALYSIS

Target audiences do not occur in a vacuum

Rather, they are created dynamically through interactions between people who share opinions, views, and interests. It is important to understand what unites members of a target audience.

Mapping stakeholders

Information influence activities are not necessarily directed at you, and they might primarily be directed towards other target groups. The most vulnerable groups in society might be the most affected. It is important to be aware of which target audiences might be vulnerable and to assess their vulnerabilities in relation to different narratives.

Map your narratives

Identify your own narratives that can be used to counter information influence activities. How can these narratives reach vulnerable target audiences? Think about which key communications officers have high credibility among vulnerable target audiences and try to reach out to them.

The purpose of implementing a target audience analysis is to develop communication tools that can be used if you are exposed to information influence activities. They are part of creating readiness with measures that can be adapted to situations where information influence activities are used to undermine your organisation's trust.

The aim of the countermeasures is to restore the damaged trust as quickly and effectively as possible. These tools include the work of preparing messages and narratives that can be directed at parts of your audience. This includes understanding how different target groups in general and key stakeholders in particular might be affected by information influence activities and how you can formulate your countermessages.

Know the organisation's risks and vulnerabilities

In addition to the above measures, organisations should also assess how information influence activities might threaten the business and the organisation's ability to fulfil its mission. A risk and vulnerability analysis is already included in the strategic planning and preparation of public organisations for different types of crises. Information influence activities could be added to existing risk and vulnerability analyses, focusing on identifying vulnerable users and other target audiences, developing finished messages and narratives, and conducting an analysis of the overall risk of information influence activities disrupting the core business.

RISK AND VULNERABILITY ANALYSIS

Step 1: Point of departure

What are your organisation's role and responsibilities?
What methods can be used to identify and assess threats and risks?
What boundaries and perspectives will be applied in the analysis?

Step 2: Risk assessment

What are the possible threats and risks?
What is the likelihood of these being realised, and what are the conceivable consequences?
What situations should be assessed in relation to the organisation's crisis-management capabilities?
What preventive steps should be taken?

Step 3: Vulnerability assessment

How is your organisation affected by different scenarios?
What consequences could the information influence activities have, and how can your organisation manage, resist, and recover from them?

Step 4: Risk management

What do you do if information influence activities are detected? See the section below for examples.

How do I choose the appropriate response?

There are no ready-made solutions that can be used to respond to all cases of information influence activities. As this handbook has shown, there are various forms of information influence activities, and not all organisations are characterised by the same vulnerabilities or prerequisites. It is therefore important to tailor the response. You can create overall frameworks for appropriate counterstrategies that fit your organisation and that can be adapted to the specific situation through thorough preparation. It is important to think about the different expectations that exist for communications officers. An appropriate response is entirely determined by your role as a communications officer and the mandate that your organisation's management has given you.

Assess, inform, advocate, or defend?

An appropriate response should be proportionate to the severity of your assessment of the situation and the threat. We propose four different degrees of response where each level includes suggestions for more specific methods.

The first level of response is about assessing the situation. This is a first step and a neutral action that also signals that you are aware of the situation and are about to find out the facts. The second level consists of informing the public and key stakeholders about the situation and how you as a representative of your organisation view the issue. This is a somewhat less neutral measure in which you report what you consider to be the facts of the case. These categories are the point of departure for a factual response and can be applied in most cases of suspected information influence.

The third level includes communicative actions where you advocate a certain position. This means that you actively argue for your own facts or message in relation to biased or false messages. The fourth level is about defending the organisation by targeting specific actions against the aggressor. These levels form the basis for a reasoned response and should be used sparingly, although they might be necessary in particularly serious situations.

Fact-based response

The first two steps in the process of countering information influence activities are assessing and informing. These are a fact-based response and can be used in any situation.

The following introduces suggestions for actions that can be used in the four steps.

STEP 1: ASSESS

To get an idea of what is going on, you need to make an assessment of the situation. What is happening? Who is involved? What is at stake? The more knowledge you can get about the situation, the better your response will be.

MAP THE SITUATION

Get your bearings and raise awareness of what is going on. Use the diagnostic tool to determine whether information influence activities are at play.

FACT CHECK

Check the information that is circulating – what is true?

TRANSPARENT UTREDNING

Get help from external actors, such as journalists, to investigate the issue in a transparent manner.

STEP 2: INFORMN

Once you have made an assessment of the situation, you can start communicating with your target audiences. In this step, your communication will focus on providing neutral information and facts, as well as communicating about how the event is being handled.Remember to always adapt your communication to the target audience.

MAKE A STATEMENT

Disclose neutral information and share relevant facts available to you.

CORRECT

Make a statement that answers or corrects a false assertion with the relevant facts. In this regard, a FAQ can be a useful tool.

REFER

In situations where external actors and experts are involved in the debate, it might be advantageous to refer to them to strengthen your position.

EMPHASISE THE VALUES

Remind your audience of what your organisation stands for.

NOTIFY STAKEHOLDERS

Disseminate information about the event to colleagues and other key stakeholders. The sooner they get to know what is going on, the better.

MAKE A PRELIMINARY STATEMENT

Show that you are working on the issue by communicating with the target audience. This gives you breathing space to elaborate a more thorough response

Argument-based response

The third and fourth steps are called argue and defend. These steps contain measures that are only appropriate in more serious situations where the information influence activities can be clearly identified. Together, they form an argument-based response.

Below you will find examples of responses in the different stages.

STEP 3: ADVOCATE

Advocacy is one step up from informing and involves more actively arguing your case. Always consider your mandate when advocating a position and remind yourself of good communication practice and your organisational values when designing your messages.

DIALOGUE

Conduct dialogue with key stakeholders and people from relevant target groups to create commitment to the issue.

FACILITATE

Make it easy for the information to reach your target audience. Organise places and times where stakeholders can meet and discuss the event or specific problems where you have the opportunity to clarify your position.

COOPERATE

Contact key players in society that can help spread your message to relevant target audiences.

PIGGYBACKING

Use existing events, initiatives, or debates to reach out with your position.

PACKAGE

Assemble an information package about the situation that presents the course of events and puts forward the facts that support your own position. It is important that the package is fact-checked and verified.

STORYTELLING

Relate the event to a broader narrative such as your organisation and your values. Make it easy for the target group to understand what is going on and to verify the information.

STEP 4: DEFEND

The final step, defend, includes a direct response to the aggressor. In some contexts the measures might appear controversial and should therefore only be used in extreme situations. Be sure to discuss all actions at this level with colleagues and managers before they are implemented so that you do not exceed your mandate or risk aggravating the situation.

IGNORE

Sometimes it is best not to do anything at all. Ignoring users or events is appropriate if it is clear that the information influence activities are present but have not been widely disseminated or noticed. In such a situation a response could instead help spread the false image.

REPORT

If an aggressor violates the law or the user rules of a media platform, it should be reported to the police or the platform owner. Notification of the platform owner must not be misused or done lightly, but only in case of obvious violations in order to avoid silencing public debate.

BLOCK

Communications officers must always be aware of the importance of respecting and maintaining freedom of expression! Activities that interfere with your business can justify blocking and suspension from a platform. However, any blocking should be justified and related to the current regulations and not related to avoiding difficult discussions.

EXPOSE

A strategic response to information influence activities might be to expose the actor who is behind it, for example, a fake account. However, this should not be done lightly and must be preceded by an impact analysis that takes into account the consequences for the organisation and for the exposed actor.

The choice of response level should be balanced against your and your management's assessment of the severity of the situation. Weak indications that an activity is a case of information influence activities are best addressed with actions that fit within the first two steps, i.e. by assessing the situation and informing the public in a neutral way. In the event of more aggressive information influence activities, the same methods can be combined with tools from the two latter response categories, i.e. with advocacy and defensive methods. However, you are advised to use caution when using the two latter steps. If you believe that the methods are justified for the specific situation, you need to ensure that you have a mandate from management to perform them and to ensure that they are consistent with democratic principles, freedom of expression, and public regulations in general.

Formulate a fact-based response

An important aspect of the first two response categories (to assess and inform) is that your communication is neutral and fact-based. If a recommending response is used, this should be seen as an additional layer. This means that the recommending response should also be based on your assessment and the facts of the matter that you have at your disposal. If incorrect information is allowed to circulate without being corrected, it might contribute to perceptions of your organisation, your target groups, or issues in your area of activity being based on inaccuracies. Assessing the situation and informing the identified target group should therefore always be the first measures.

In order to conduct a relevant fact check, you first need to consider how incorrect information can affect your organisation, how it risks influencing your business, and how you go about identifying it. Who is spreading the information, how far has it spread, and what is the topic? For example, organisations can focus on evaluating the articles that contain quotations from the organisation's representatives, posts that become viral and widely spread online, or claims about their own organisation and its field of activity. By collecting the facts in a systematic manner, you can ensure that you evaluate the information and questions that you deem relevant to your area of responsibility.

Evaluation

- ☑ Obtain neutral expert opinions and/or accurate information from relevant and reliable sources
- ☑ Ask for more information from the person or organisation that made the claim
- ☑ Locate the original source of the false claim

If the information is deemed incorrect, you should first respond with a correction. Many experts believe that disinformation is best met with accurate information. Others say that the message only has an effect among those who are interested in finding out the truth. Your preparatory work with target audiences and narratives creates opportunities for an informed assessment of which action is appropriate in each specific case.

Remember that if you have the option and the mandate to make an argument-based response, it should follow the framework established within the fact-based response.

Formulate a fact-based response

- ☑ Ask the person who posted the error to correct or withdraw the publication.
- ☑ Prepare a fact sheet or similar document that is easy to share online.
- ☑ Try not to repeat the incorrect information in your communication.
- ☑ Remember that not all incorrect information must be addressed.
- ☑ Question the context of the debate, not just the content.
- ☑ Consider conducting a dialogue as a complement or alternative to your prepared communication.

Special considerations for social media

Social media are not just platforms that allow users to interact with each other, and they can also be used as a tool for information influence activities. Social media have their own logic, which users need to know, understand, and take into account in any countermeasures against information influence activities.

It can be difficult to know who is behind an account on social media and where the information comes from. The discussion might, for example, claim to represent public opinion on false grounds. Social media are challenging because information can be spread quickly. It is necessary to take account of elements such as tags, name calls, links, and attachments. A typical post on social media contains one or more of these elements, which also connect the message to other accounts, ideas, and debates. In this way, the post should be considered part of one or more larger networks of on-going conversations online.

TAGS

Create a keyword for a post. Tags often affect the spread and circulation of posts.

NAME CALLS

Used to link to an organisation or an individual's account so that they receive a notification about the post.

LINKS

Provide a hyperlink to another website. Links are often abbreviated so that the website's real URL is not visible.

ATTACHMENTS

Multimedia files, such as an image or video clip. These can change the meaning of a post and should not be overlooked.

Proactive work on social media means building networks and tags that ensure that the organisation's communication reaches the right people. As a communications officer, you should prepare messages that can be pre-approved and used in the event of a crisis. In this way, you can give a quick response in cases where you need to counter information influence activities. Social media also make it possible for an organisation to detect, in real time, any threats or vulnerabilities related to the reputation of the organisation. In this way, social media can be used both as a tool for dialogue and as an open analysis tool to understand key trends and contemporary directions in public debate.

Countering influence on social media

The four response levels form a toolbox to counter information influence activities. The following is an example of how the tools can be applied to counter influence on social media.

ASSESS

Assess the situation using your knowledge of information influence activities. Is it about influence or is it engaged citizens who are debating? If you suspect that information influence activities are taking place, map the situation as carefully as possible. Which users are communicating with you? Are they hostile to you or are they reacting to something that has been spread with the aim of creating hostile reactions? What tags are being used? Are there attached links or other materials? What sources are being referred to? Are any accounts bots? A quick assessment lays the foundation for action.

INFORM

Formulate your message based on your assessment. Carefully choose which audiences you want to reach first, and identify the users and hashtags you can use. Focus on reaching out with neutral information and emphasise the organisation's values in the channels you consider appropriate.

RECOMMEND

If you think it advisable to move on to the recommend level, you can use the available tools to position yourself more clearly in the debate, for example, through prepared messages or multimedia. It might also be advisable to participate more actively in the debate and to create broader commitment to the issue among your target groups. This is achieved by communicating directly with other users and involving followers in the debate.

DEFEND

f the situation escalates to a position where constructive dialogue is impossible and messages are pushed aside by spam and destructive posts, it might be advisable to go into a defensive position. Depending on your organisation's policies and the platform's rules, you might be allowed to block or ignore offending users. Always consult managers and colleagues before you act! Freedom of expression is one of the core values of our society, and we must always do what we can to maintain open and free democratic debate. If you decide to block or ignore a user, make sure to be completely transparent about the reason for your decision.

How do I make use of lessons learned?

Collecting and documenting examples of information influence activities is central to understanding the problem better and thus being better able to counter such activities in the future. Examples of responses you have provided and assessments of whether the response worked are important to document for later use to create a log of the course of events with information about actions and timings and to design procedures and ways of working for possible future attempts to exert influence. Knowledge can also be used to develop educational materials and streamline organisational and societal preparedness. The information should be shared with communications officers in similar roles, authorities with the task of identifying and addressing information influence activities (e.g. MSB), and in some cases with the public.

On the next page, there are some examples of lessons learned that you should save and have on hand when you respond to information influence activities.

Lessons learned

BESKRIV

- ☑ Describe the background, progression, and context of the event.
- ☑ Which actors were involved? (avoid speculation about sources when you do not know).
- ☑ Which of the distinctive characteristics of information influence activities could be observed?
- ☑ What vulnerabilities were exploited?
- ☑ Which influence techniques were used? Which target groups and narratives were used?
- ☑ Does the event fit into a broader context?

REFLECT

- ☑ What effect do you think the aggressor wants to achieve? What is your assessment based on?
- ☑ How did you act? Reflect on what actions you took and why you chose them.
- ☑ What do you think would have happened if you had not acted?
- ☑ What effect did your actions have?
- ☑ What worked well and what could you have done differently?
- ☑ What lessons can you learn from the event?

SHARE

- ☑ Have you saved evidence or data related to the case?
- ☑ Discuss the information influence activities with your managers and colleagues and share your experiences.
- ☑ Maintain regular contact with colleagues inside and outside your own organisation who work on similar issues.
- ☑ Share your knowledge and experience within and outside your own organisation, for example, through training and meetings.

Strategic considerations

Your response is limited by the fact that it always responds to someone else's agenda. The aggressor might seem to set the conditions, which means that the whole principle of countering information influence activities is problematic. It often feels like they act and you react and that you are constantly one step behind your opponent's last move.

It might therefore be more sensible to focus on actions that defend democratic values such as free debate and freedom of expression. Your mission is to protect the opinion-formation process in relation to your organisation's mission by minimising the impact of vulnerabilities in the media system and in opinion-forming and human thought processes. Here, it is important that you proceed from strategic, well balanced, and at the same time fact-based responses.

It is worth reiterating that the work of countering information influence activities must never lead to public debate being silenced. This would be counter to the very purpose of countering information influence activities, lead to increased polarisation, and undermine the functioning of society. Open and democratic debate must always be protected and encouraged.

- ☑ Raise the threshold for information influence activities by contributing to awareness and preparedness
- ☑ Develop proactive, balanced, and sensible communication methods that focus on the target group (rather than the opponent) and defend society's shared values
- ☑ Maintain a fact-based response, which can develop into a recommending response in certain circumstances
- ☑ Share methods that work, and learn from each other.
- ☑ Be vigilant, but not paranoid!

Glossary

Bandwagon effect – That people who feel they are part of a majority are more likely to share their opinion.

Bots – Computer programs that perform automated tasks.

Disinformation – Incorrect or manipulated information that is deliberately spread in order to mislead.

Dark ads – Advertisements that can only be seen by specific individuals with messages tailored to the individual's psychographic profile.

Echo chambers and filter bubbles – Organic groupings online or offline where people communicate with others who share the same views and beliefs.

Fake media – Forged news sites designed to mimic true news sites.

Hacking – When actors acquire unauthorised access to a computer or network.

Straw man – To ascribe to opponents arguments and positions the opponent does not stand for, and then to argue against these positions instead of the opponent's actual positions.

Shilling – People who give the impression of being independent but who actually work with or receive payment from someone else.

Memes (also called Internet memes) – Refer to images, phrases, activities, concepts, or films, often with humorous content, that are spread on the Internet, mainly via social media.

Phishing – Users are tricked into providing their passwords or other sensitive information on the Internet.

Potemkin villages – Fake companies, research institutes, and think tanks that are used for disinformation to be perceived as information.

Sock puppets – Fake accounts used to participate in online debates where two or more sock puppets are used to fire up the discussions.

Strategic narratives – Stories designed to support a specific purpose.

Symbolic acts – Acts performed primarily to communicate a message.

A spiral of silence – People who feel they are part of a minority are less likely to share their opinion.

Whataboutism – To take the focus from an argument by highlighting a similar phenomenon that has not received as much attention, but which is not really relevant to the issue.

More information

This handbook and a full bibliography are available on the MSB website:

https://www.msb.se

If you would like to learn more about information influence activities, we recommend that you read this handbook. You can also find more information in the following reports and articles:

Countering Information Influence Activities: The State of the Art,
Pamment J., Nothhaft H., Twetman, H. & Fjällhed A., 2018

Att förbygga och hantera påverkansförsök – en handbok
Brottsförebyggande rådet (BRÅ), 2017

Källkritik på internet
Internetstiftelsen i Sverige (IIS), 2016

Personlig säkerhet
SÄPO, 2018

Debunking handbook
John Cook och Stephan Lewandowsky, 2012

Alternativa fakta – om kunskapen och dess fiender
Åsa Wikforss, 2017

Participatory propaganda: the engagement of audiences in spread of persuasive communications
Alicia Wanless och Michael Berk, 2018

Theoretical Fondations of Influence Operations: a review of relevant psychological research
Björn Palmertz för MSB, n.d.

The Russian 'Firehose of falsehood' Propaganda Model – why it might work and options to counter it
Christopher Paul och Miriam Matthews för RAND, 2016

You can also access information and examples from other international organisations:

EU vs Disinfo
www.euvsdisinfo.eu

The European Center of Excellence for Countering Hybrid Threats
www.hybridcoe.fi

NATO Strategic Communications Centre of Excellence
www.stratcomcoe.org

Swedish Civil Contingencies Agency (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.no MSB1260 - December 2018 ISBN 978-91-7383-910-5