Swedish Civil
Contingencies
Agency

Countering information influence activities

A handbook for communicators

Countering information influence activities

A handbook for communicators

Countering information influence activities – A handbook for communicatiors

Swedish Civil Contingencies Agency (MSB)

Layout: Advant

Order No: MSB1263 – March 2019 ISBN: 978-91-7383-867-2

This publication is also available in Swedish
Att möta informationspåverkan – Handbok för kommunikatörer
Order. No: MSB1260 – Revised December 2018 ISBN: 978-91-7383-864-1

Content

Foreword

The deteriorating security environment has increased the need for the Swedish authorities to become more knowledgeable about how to identify, understand, and counter information influence activities. Influence campaigns have become increasingly sophisticated and can be used in times of peace and war. This affects the role and responsibilities of our government authorities.

Information influence activities can disrupt the way our society functions by exploiting vulnerabilities and challenging the values that are fundamental to our way of life such as democracy, the rule of law, and human rights—ultimately endangering the life and health of our people. Safeguarding the democratic dialogue—the right to open debate, the right to arrive at one's own opinions freely, and the right to free expression—is paramount as we work to lay a solid foundation of social resilience to counter information influence activities.

The Swedish government has resolved that our public officials should be able to identify and counter information influence activities and neutralise propaganda campaigns. The Swedish Civil Contingencies Agency (MSB) has been working actively since 2014 to develop our capacity to identify, understand, and counter hostile information influence campaigns. Increasing public awareness is central to countering information influence.

Agencies responsible for our national security have expressed the need for a manual describing the principles and methods of identifying, understanding, and countering information influence activities. Therefore, in collaboration with researchers at Lund University, MSB has produced this handbook, which is directed primarily toward communicators working in public administration. It should be considered supporting material for situations when an organisation suspects it has been exposed to an information influence campaign or is at risk of such an attack.

I would like to thank the Department of Strategic Communication at Lund University whose research is the basis for the handbook. Special thanks also go out to the agencies and organisations that have contributed to improving this handbook with their wise comments and experience, making it a more useful resource.

Dan Eliasson, Director General

Introduction

Introduction

This handbook was created in response to the deteriorating security situation in the world today. The illegal annexation of Crimea and the conflict in Ukraine have shown how 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 Sweden's national security – including the life and health of our population, the functioning of society, and our ability to preserve fundamental values such as democracy, the rule of law, human rights, and other fundamental freedoms.

The MSB 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 Swedish public decision-makers, the opinions of all or a part of the Swedish population, and opinions or decisions taken in other countries that might adversely affect Sweden's sovereignty, security, or other interests.

An influence campaign consists of a number of influence activities, one of which is information influence. This handbook will help you as a communicator to become more aware of what information influence activities are so you can more easily identify and counter this type of security threat.

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. There are a number of cases from around the world where such influence activities have been identified, for example the recent presidential elections in the US (2016) and France (2017). While these are aggressive acts, they are not considered acts of war, even if they sometimes are described as operating in the grey zone between war and peace. Information influence activities should be considered hostile as they undermine public confidence in important social institutions, isolate vulnerable communities, and contribute to social and political polarisation.

Our society is built on trust—on public confidence in our social institutions and on trust between the people and communities that make up our society. Trust and confidence are essential to a well-functioning democracy. Information influence activities erode trust by sowing doubt and exploiting divisions. When foreign actors use influence techniques against a population it may represent a threat to national security. The ability to maintain confidence and respond appropriately to information influence activities with fact-based, trustworthy messages is essential for a resilient, healthy democratic society.

What is the role of the communicator?

As a communicator you have the opportunity to play an important role in preventing, identifying, and countering information influence activities. You help your organisation keep its promises and build a trustworthy relationship with the public. You communicate with your target audiences, answer their questions, and provide them with vital information. As a communicator, you know what your audiences think and what is important to them.

It may seem unlikely, but one day even your organisation may become the target of information influence activities. For example, you may discover that false information is being spread about your organisation, a fake version of your website has appeared, or your social media accounts have been hacked. Your organisation's target audiences may become the targets of cyber-bullying, trolling, or disinformation. The goal of such attacks may be to undermine confidence in your organisation, introduce false or misleading information into important debates, or increase tensions between your target audiences. In all of these cases, you have the opportunity to play an essential role in strengthening and supporting productive democratic debate.

WHY DO COMMUNICATORS MATTER?

- You build bridges between your organisation and the public.
- You already have experience with other forms of crisis communication that will be relevant when responding to information influence activities.
- You may be among the first to encounter information influence activities as they occur.

As a communicator you already have many of the skills needed to counter information influence activities. This handbook provides additional information to support you in this work. You will learn which techniques may be used against you and how to spot the warning signs. You will receive advice on how to prepare your organisation for a quick and effective response, and guidance about how to choose the best response for your organisation based on your unique circumstances and your mandate as a communicator.

Our approach

The purpose of this handbook is to increase your awareness and understanding of information influence campaigns and develop your ability to respond. The information given here will help you recognise common influence techniques more easily and provide you with a toolbox of proactive solutions you can use to design the most appropriate response. This handbook does not provide a one-size-fits-all solution or a checklist of steps to tick off. Each organisation is different, communicates with different audiences, and faces different challenges that must be considered when deciding how best to respond.

PART I: BECOMING AWARE OF INFORMATION INFLUENCE

What are information influence activities?

How do they exploit social vulnerabilities?

How are information influence activities different from other forms of communication?

PART II: IDENTIFYING INFORMATION INFLUENCE

What is the purpose of information influence activities?

What are the main information influence techniques?

How can these techniques be combined?

PART III: COUNTERING INFORMATION INFLUENCE

How do I prepare my organisation?

How do I choose an appropriate response?

How do I ensure that lessons are learned?

PART I.
Becoming aware of information influence

What are information influence activities?
How do they exploit social vulnerabilities?
How are they different from other forms of communication?

PART I. Becoming aware of information influence

This section describes how information influence activities exploit societal vulnerabilities and provides tools for assessing suspicious activity and identifying cases of information influence.

What are information influence activities?

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 that rely upon informed consent. They should be met with facts, source criticism, and a commitment to the public interest.

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 in a new way.

Information influence activities involve potentially harmful forms of communication orchestrated by foreign state actors or their representatives. They constitute deliberate interference in a country's internal affairs to create a climate of distrust between a state and its citizens. Information influence activities are used to further the interests of a foreign power through the exploitation of perceived vulnerabilities in society. Foreign state actors study the controversies and challenges of a society and exploit these vulnerabilities to disrupt and polarise.

Information influence activities may be deployed separately or carried out as part of a larger influence campaign, drawing on a broad spectrum of techniques. In addition to communications tools, everything from diplomatic and economic sanctions to demonstrations of military force can be used to influence society.

ANATOMY OF AN INFORMATION INFLUENCE CAMPAIGN

Using influence techniques
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.

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.

How are social vulnerabilities exploited?

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. This is where you can play an important role.

Opinion formation

NEW INFORMATION
New information reaches us: an event, scientific discovery, media disclosure, or political decision.

EXPERTS, OFFICIALS AND SOURCES
This new information is documented by witnesses, experts, and officials who explain or interpret it for others.

MEDIA AND CULTURE
Newspapers, television, radio, blogs, and social media are used to communicate the message to the public.

THE PUBLIC
Information reaches the public and is processed both through discussion and dialogue among various social groups, both face-to-face and on social media.

YOU
Information reaches you through the communities you belong to and the information channels you consume.

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.

How are information influence activities different from other forms of communication?

It is not the role of the communicator to investigate whether foreign power is responsible for specific communication activities. You are only expected to act when you suspect that information influence activities are being used in relation to the work you do, or to undermine the integrity of public debate and Sweden's national security. Use your best judgment to make an assessment. In other words, it is important that you understand the role your organisation plays from a social perspective, in a wider context.

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.

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.**

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.

PART II. Identifying information influence

What is the purpose of information influence activities?
What are the main information influence techniques?
How are these techniques commonly combined?

PART II. Identifying information influence

Identifying information influence activities is the first step towards countering them. This means knowing what to look for. In this section, we provide guidance for assessing strategic narratives and audience targeting approaches and more detailed descriptions of the techniques used in influence activities. Then we discuss how these techniques may be combined to produce negative social effects.

What is the purpose of information influence activities?

To successfully identify information influence activities, you must also be aware of strategic narratives and target groups. Basic awareness of these concepts and their meaning will help you better understand and identify suspected cases of information influence activities and give you some insight into the possible intention behind an activity.

Strategic narratives

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, or 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. Consider the three approaches below. Can you identify a strategic narrative that uses one of these approaches?

STRATEGIC NARRATIVES

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 audiences

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.

TARGET GROUPS

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.

In conjunction with an analysis of the strategic narratives and communication techniques being used, target audience analysis can reveal the intent of information influence activities. If you understand *who* is being targeted and *why*, it will be easier to make a reasonable assessment of *what* the purpose of the information influence activities are. This in turn will help you decide *which counter measures are most appropriate*.

What are the main information influence techniques?

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.

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

TECHNICAL EXPLOITATION
- Bots
- Sockpuppets
- Deepfakes
- Phishing

DISINFORMATION
- Fabrication
- Manipulation
- Misappropriation
- Satire and parody

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

SYMBOLIC ACTIONS
- Leaking
- Hacking
- Public demonstrations

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.

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.

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.

HEADLINE

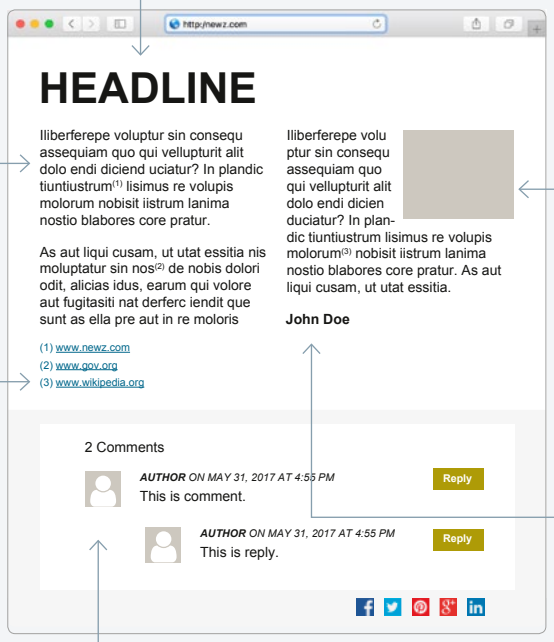
Headlines aspire to generate interest and a response from the reader. Keep reading beyond the headline to make sure that it matches the content of the article.

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.

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.

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.

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 sockpuppet 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

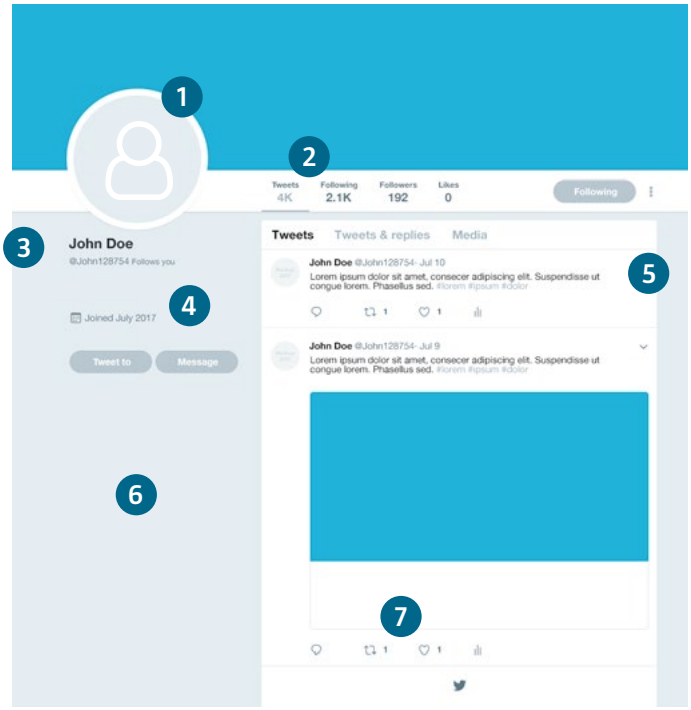
Advanced machine learning algorithms can now be used to manipulate audio and video very convincingly, for example of a real politician delivering a fictitious speech. It is even possible to superimpose the face of another person onto pre-existing video footage and digitally reconstruct a person's voice.

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. Spam-bots, 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, some- times 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.

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.

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.

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.

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.

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.

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).

How are these techniques commonly combined?

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. Your assessment should therefore consider whether there is evidence of multiple, coordinated actions directed at your organization. On the following page, we offer some examples of what coordinated influence activities might look like.

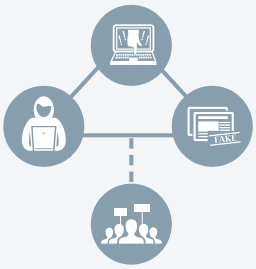
We suggest a number of questions you can use to help you assess communications and identify information influence activities. What narratives can you identify and who are they aimed at? Is there any evidence of an intention to deceive or disrupt? Do you suspect interference from a foreign actor or proxy? Do you see a combination of techniques suggesting a coordinated effort or campaign against your organisation? If you find there are grounds for concern, the next section contains suggestions for how to respond.

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.

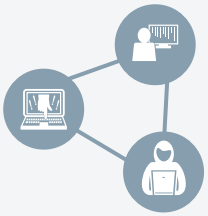
Polarisation

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.



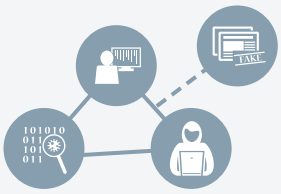
Laundering

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.

PART III. Countering information influence

How can I best prepare my organisation?
How do I choose the most appropriate response?
How do I ensure lessons are learned?

PART III. Countering information influence

In this section, we will discuss how to counter information influence activities. We will help you prepare your organisation to meet this threat, discuss actions that can be taken when an attack is underway, and suggest how best practice should be shared to promote organisational learning.

PREPARE

Raise awareness
Build trust
Assess risks

ACT

Choose your response
Check your facts
Use social media

LEARN

Describe
Reflect
Share

How do I prepare my organisation?

Preparation is the most important part of any crisis management plan. 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: 1) sharing information and raising awareness, 2) understanding of how your key audiences and stakeholders may be vulnerable to information influence activities and developing narratives and messages around potential problems, and 3) carrying out a risk and vulnerability analysis for your organisation.

Raising 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.

As a communication professional in a public sector organisation there are several things you 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 organisation to prevent the spread of disinformation.

Building trust through strategic communication

One of the goals of information influence is to undermine trust between people and social institutions. 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 public institutions is an important aspect of any counter measure strategy.

Prepare messages

Since it may take time for messages to be prepared and approved during a crisis, it is important to prepare generic messages that assert your organisation's values, and can be readily adapted to a specific event. Just as organisations use targeted messages to describe a new initiative or product, they can also be used to raise awareness of fake stories and to refute them.

PREPARED MESSAGES

Quick, accurate responses on social media are made possible by solid preparatory work—prepare crisis response messages in advance with the approval of upper management. For example, the Metropolitan Police in London sent its first tweet just seven minutes after the Westminster terrorist attack of March 2017. The tweet provided accurate information about the unfolding situation but was based on a generic message prepared for similar scenarios that could quickly be adapted to the current events.

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.

WHAT'S YOUR STORY?

Messages should be aligned with the overarching narrative you want to project.

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

Analysis and understanding which factors contribute to your organisation's preferred narratives simultaneously builds an understanding of your organisation's reputational vulnerabilities.

Any attack is best countered by upholding those values your organisation stands for.

Know your public

Clearly establishing the core values, messages, and preferred narratives for your organisation is fundamental to understanding your vulnerabilities and which stakeholders are at greatest risk for information influence. If an influence campaign has been detected, these are the groups to reach out to first.

As a professional communicator, you already have experience of conducting target audience analysis. The difference here is that you are asking which audiences are most vulnerable to information influence and why. Identify which areas of your organisation are most likely to be subjected to information influence activities and consider what type of malicious messaging they might be susceptible for. When this has been done you can prepare suggestions for how to reach these key audiences with preventative information and counter-messages.

TARGET AUDIENCE ANALYSIS

Key audiences do not exist in a vacuum

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

Identify your stakeholders

Information influence activities may not necessarily be directed at your organisation but may primarily be directed towards other target groups associated with you. The most vulnerable groups in society can be the most affected. It is important to be aware of which target groups are at risk and to assess their vulnerabilities in relation to different narratives.

Design your core narrative

Identify narratives that can be used to counter information influence. How can these narratives reach vulnerable target groups? Include key communicators with high credibility as possible intermediaries for reaching out to those groups

The purpose of doing a target audience analysis is to develop communication tools that can be used should you be subjected to information influence activities. This is a form of contingency planning that can be adapted to situations when information influence methods are used to undermine your reputation.

The counter-measures discussed here are meant to help you restore trust as quickly and effectively as possible. They include prepared messages and narratives that can be directed to different key audiences and stakeholders in your organisation. To prepare these messages you must first understand how the different audiences might be affected by disinformation and how best to design messages for each audience.

Know your organisational risks and vulnerabilities

In addition to the above, your organisation should prepare a formal assessment of how information influence activities can threaten its ability to fulfil its mission. Public sector organisations include risk and vulnerability analyses in their strategic planning and crisis preparations. We suggest adding information influence activities to existing risk and vulnerability analyses, with a specific focus upon vulnerable stakeholders/audiences, key values, messages and narratives, and the overall risk to your organisation's core activities.

RISK AND VULNERABILITY ANALYSIS

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?

Step 4: Risk management
What should be done if information influence activities are identified?
See the below for examples.

How do I choose the best response?

There is no one-size-fits-all response to information influence activities. As this handbook has shown, the information influence activities can vary greatly. More importantly, your organisation operates under unique conditions and has its own specific vulnerabilities. With thorough preparation, you can create a general framework for countermeasures that suit your organisation and can be adapted to a variety of situations. Consider your role as a communicator, the expectations placed upon you, and the mandate you have been given by your organisation's leadership to determine the best response for each situation.

Assess, inform, advocate or defend?

An appropriate response will be proportionate to the threat. We suggest four categories of response, each consisting of a number of communicative techniques.

Fact-based: 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 organisation sees it. This is a slightly less neutral response that outlines what you consider to be the facts of the case. These actions are the building blocks for any further rational, fact-based response and can be applied to most cases of suspected influence activities.

Advocacy-based: 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 organisation by taking specific actions against the aggressor. These levels are the basis of an advocacy-based response. While they may be appropriate, they should always be used with caution depending on the severity of the situation.

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

AAnalyse 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

The third and fourth levels are to advocate and defend. These steps contain measures that are only appropriate in severe situations where an information influence campaign has been clearly identified. Together these make up an advocacy-based response.

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

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

SSometimes 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.

Choosing the most appropriate level of response depends on your assessment of the severity of the situation. A suspected case of information influence with only weak indicators is best addressed at levels one and two, i.e. **assess** the situation and **inform** the public in a neutral manner. This is a *fact-based respons*e. For a more aggressive case of information influence use the fact-based methods of levels one and two in conjunction with the more assertive of levels three and four, i.e. **advocate** your position and **defend** your organisation against the attack. This is an *advocacy-based response*. However, use caution at these levels. Ensure you have a clear mandate from your leadership and that your response is consistent with democratic principles and freedom of expression, as well as other regulations and codes of conduct that may apply.

Developing a fact-based response

The most important aspect of the first two response levels is that your communication must be neutral and based on facts. These two qualities define a fact-based response. **An advocacy-based response should be considered a second layer that always builds upon the first compulsory, fact-based layer.** If inaccurate information is allowed to circulate without correction, this can contribute to the perception that your organisation, its key audiences, or its core issues are built on mistakes and falsehoods. Therefore, assessing the situation and informing identified key audiences must always be the first response.

In order to ensure that any fact-checking you do is relevant, you must first understand how false information affects your organisation, how it can undermine your activities, and to identify it. Who is spreading the disinformation? How widely has it spread? Which topics are concerned? One approach is to focus on articles featuring quotes from your organisation's representatives, relevant stories that have gone viral online, or public claims about your organisation and its area of operation. Collecting facts systematically so you can evaluate the questions that are relevant to your area of responsibility.

Assessment

- ☑ Collect neutral expert opinions and/or accurate data from relevant and credible sources.
- ☑ Request more information from the person or organisation making the claim.
- ☑ Find the original source of the false data.

If the information is deemed false, providing a correction is appropriate. Many experts believe that disinformation is best countered by accurate information. However, some argue that you will only reach those interested in discovering the truth. Your preparatory work on key audiences and narratives should help you determine how to respond in each case.

If you have the option and the mandate to develop a persuasive advocacy-based response, it should be based on the lines established in the fact-based response.

Developing a fact-based response

- ☑ Request a retraction or correction from the author/ publisher of the falsehood.
- ☑ Prepare a fact sheet or similar document that can be shared easily online.
- ☑ Be cautious of repeating false information in your communications.
- ☑ Remember that not every piece of false information needs to be corrected.
- ☑ Question the premise of the debate, not just the content.
- ☑ Consider engaging in dialogue as a supplement or alternative to your prepared communications.

Special considerations for social media

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.

TAGGING

creates a search term for a post. Tags influence the circulation and reach of a post.

NOTIFICATIONS

activate a link to an individual or organisational account to notify them about posts of interest

LINKS

provide a hyperlink to other websites. Links are often abbreviated so the full URL is not visible.

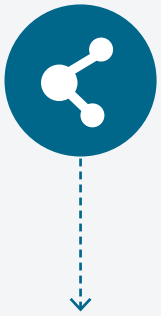
ATTACHMENTS

include multimedia files such as an image or video in a post. Note that they can change the meaning or intention of a post and should not be overlooked.

Proactive social media work includes building networks and establishing hashtags that enable an organisation to reach the right people with their messages. Generic posts for handling crises can be prepared and cleared beforehand, ensuring a prompt response when an unforeseen event occurs. Social media also enable an organisation to discover potential threats or vulnerabilities to its reputation in real time. It is therefore an advocacy tool for dialogue and messaging, and an open source intelligence tool for understanding important trends.

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.

How do I ensure that lessons are learned?

It is crucial to collect and document examples of information influence activities to further our understanding of the problem. Furthermore, to establish best practices for your organisation it is essential to document your responses and assess their success in achieving the desired effect. Use your examples to develop a log of events as they unfolded and design proactive routines for possible future attacks. You can also develop training materials to streamline your organisational approach and contribute to societal preparedness in general. Share your knowledge and experience with communicators in similar roles, and with public authorities tasked with identifying information influence activities (e.g. MSB in Sweden), and in some cases, with the public.

On the next page we have provided some examples of the type of information you should save in cases of suspected information influence:

Learning

DESCRIBE

- [x] Describe the background, progression, and context of the event.
- [x] Which actors and networks were involved? (Avoid speculation if you don't know.)
- [x] Which characteristics of information influence activities did you observe?
- [x] Which vulnerabilities were exploited?
- [x] Which influence techniques were used? Which audiences and narratives were used?
- [x] Does the case fit into a broader pattern of activities?

REFLECT

- [x] What do you think where the intended effects? On what do you base your assessment?
- [x] How did you act? Reflect on the steps you took and the choices you made.
- [x] What do you think would have happened if you did not act as you did?
- [x] What were the effects of your response?
- [x] What did you do well and what would you do differently?
- [x] What have you learned from this experience?

SHARE

- [x] Have you saved evidence or data related to the case?
- [x] Discuss information influence activities with your organisation's leadership and colleagues and share your experience.
- [x] Maintain regular contact with colleagues working on similar issues within your organisation and in other organisations.
- [x] Share your expertise and experience with others both within your organisation and with other colleagues by participating in meetings and educational events.

Strategic considerations

Any attempt to counter an influence activity is limited by the fact that you are respond to somebody else's agenda. The aggressor seems to set the conditions, which means that countering information influence activities is problematic. It can feel as if they act and we respond, that we are always a step behind the latest attempts to exploit our social vulnerabilities.

Therefore, it makes more sense to focus on upholding democratic values such as open debate and freedom of expression. Your mission is to protect the process of independent opinion formation as it relates to your organisation by minimising the effects of vulnerabilities in the media system, public opinion, and human cognitive processes. It is important to start from a strategic, balanced, fact-based position.

It is worth repeating that efforts to counter information influence activities should never silence public debate. This would be counter-productive and only lead to further polarisation and undermine the principles our society is based on. Open and democratic debate must always be protected and encouraged.

- ☑ Raise the threshold for information influence activities through awareness and preparation.
- ☑ Develop proactive, proportionate, and sensible methods of communication that focus on key audiences (rather than an adversary) and defend the values we share.
- ☑ Maintain a fact-based response that can be developed into an advocacy-based response under certain circumstances.
- ☑ Sharing best practices and learn from each other.
- ☑ Be vigilant but not paranoid!

Glossary

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 villages – 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 the 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.

Further reading

This handbook is based on the 2018 report *Countering Information Influence Activities: The State of the Art* by Pamment, Nothhaft, Twetman, and Fjällhed.

You can find the report along with a full reference list on MSB's website: https://www.msb.se

We also recommend the following reports and articles as helpful resources:

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 draw 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)
SE-651 81 Karlstad Phone +46 (0)771-240 240 www.msb.se/en
Order No. MSB1263 - March 2019 ISBN 978-91-7383-867-2