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 communicators

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

Swedish Civil Contingencies Agency (MSB)

Layout: Advant Produktionsbyrå

Order No: MSB1263 - July 2018
ISBN: 978-91-7383-867-2

Table of content

Foreword

The Swedish constitution reflects the society in which we live – a society that safeguards the fundamental freedoms and rights of all citizens. These freedoms and rights are foundational, and their protection is the key to maintaining a democratic and open society.

In recent years, the Swedish government has emphasised that Sweden must have the ability to handle a new kind of national security risk: information influence campaigns conducted by foreign powers. Information influence campaigns are antagonistic acts that threaten our democracy and our sovereign decision-making.

The Swedish Civil Contingencies Agency (MSB) has been working actively since 2014 to develop Sweden's capacity to identify, understand and counter hostile information influence campaigns. Increasing the public awareness is central to countering information influence campaigns.

To help achieve this, MSB has collaborated with researchers at Lund University to produce this handbook. The handbook aims to assist and support communication specialists in public administration to identify, analyse and counter information influence activities in order to mitigate their impact on society. A central principle for all activities described in this handbook is that they always comply with Swedish laws and principles on freedom of expression and freedom of the press, on which our democracy is founded.

Free and fair elections are a central part of our democratic system. Thus, any attempt to influence these elections is by extension a threat to our democracy. On the basis of observed information influence campaigns targeted at disrupting democratic elections in other countries, MSB has concluded that parts of Swedish society are potential targets for hostile influence aimed at the upcoming elections. Therefore, general awareness regarding threats, methods and available counter-measures must permeate all levels and all sectors of public administration before, during and after the 2018 elections.

Finally, MSB would like to express appreciation to the team of researchers at Lund University under the leadership of Dr. James Pamment on whose research the handbook is based.

Introduction

Introduction

The annexation of Crimea and the conflict in Ukraine has shown how security threats today can assume a radically different character than what we usually associate with international conflict. There, means other than traditional military means were employed to achieve specific strategic goals. Influence campaigns is the term used to describe this new type of security threat. In influence campaigns, foreign powers exploit societal vulnerabilities to achieve their goals without the need for military force. Influence campaigns are a phenomena that we need to defend ourselves against to safeguard the goals of Sweden's security; the life and health of our population, the functionality of society, and our ability to preserve fundamental values such as democracy, 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, to influence political and public decision-making, public opinion, or opinions in another country, which may affect Sweden's sovereignty, the goals for Sweden's security or other Swedish interests negatively. An influence campaign consists of several influence activities, of which information influence is one. This handbook helps you as a communicator to become aware of what information influence is, how it works, and what you can do to counter this type of threat.

The use of information to influence others is not new. Industries such as public relations and advertising use information to influence the personal decisions of people around the world every day, such as the choice to buy a certain brand or to support a political candidate. We, as citizens, expect such communication to take place in the open, to be based on accurate and truthful information, and to be presented in a way that allows us to make informed choices.

Not all influence activities play by these rules. Information can be used covertly and deceptively by foreign powers to undermine processes critical to the fabric of democratic societies. This is what we refer to as information influence activities. There are many contemporary examples from around the world where such activities have been identified, as in the recent presidential elections in the U.S. and France. From a big picture perspective, these activities are part of how countries vie for influence in international affairs. They are hostile activities but not acts of war. Indeed, they are still sometimes referred to as information warfare, or as operations taking place in a grey zone between war and peace. They are still considered hostile as they often intend to undermine public confidence in critical societal institutions, isolate vulnerable communities, and contribute to social and political polarisation.

The cornerstone of societal cohesion is trust. Information influence activities erode trust in social institutions and between social groups. They exploit doubt and sow division. When foreign state actors use these techniques against a population, it could represent a threat to national security interests. Consequently, maintaining trust between social institutions and the people they serve is a critical component of national security. The ability to counteract information influence activities with trustworthy communicative responses is essential to a resilient, healthy democratic society.

What is the communicator's role?

As a communicator, you can play a key role in identifying and countering information influence activities. You know your audiences and what's important to them. You talk regularly with them, prepare information for them, answer their questions and alleviate their concerns. You deal with crises big and small and ensure that trust never breaks down even under the most extreme pressures. You help your organisation deliver on its promises and have your finger on the pulse of population.

Although it may seem unlikely, it is possible that your organisation will one day become a target of information influence activities. For example, you may be subjected to disinformation, fake versions of your websites and hacked social media accounts. You may notice that a part of the population is being targeted by trolls, hate speech or misleading content. The effect of such attacks may be to undermine reputations, introduce falsehoods into important debates, or increase tensions between social groups. In all cases, communicators have an essential role to play in strengthening and supporting a productive democratic debate.

WHY COMMUNICATORS?

- You bridge the gap between your organisation and its publics.
- You handle other forms of crisis communication for your organisation.
- You may be among the first to encounter information influence activities as they occur.

As a communicator you already possess most of the skills that you will need to counter information influence activities. This guide provides a crash course in the additional things that you need to know. It will teach you about the techniques that may be used against you and how to spot warning signs. It will give advice about how to prepare your organisation for an effective response. It will support your ability to make the best decisions for your organisation and your constituents, based on your responsibilities and your mandate.

Our approach

The purpose of this guide is to help you as a communication professional in public administration to identify and counter information influence activities. We aim to increase awareness and understanding of the issue, enable recognition of common techniques, and make available a toolbox of proactive communicative responses. We do not provide a one-size-fits-all solution, or a single checklist that you can tick off. Each organisation is different, speaks to different parts of the public, and faces different challenges. With this text, we aim to support and develop your ability to decide upon the best possible response to information influence activities.

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 do these components fit together?

PART III: COUNTERING INFORMATION INFLUENCE

How do I prepare my organisation?
How do I choose an appropriate response?
How do I make sure that lessons are learned?

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 I. Becoming aware of information influence

In this section, we will explain how information influence activities exploit societal vulnerabilities and provide a tool for assessing suspected information influence activities.

What are information influence activities?

Open debate, differences of opinion, and efforts to persuade others are essential features of a healthy democratic society. But what happens when falsehoods are introduced into the discussion? What happens when somebody produces manipulated evidence, employs fake experts, or makes deliberately misleading arguments? Such communications 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 have healthy and vibrant political participation from people who see it as their role to correct illegitimate communications and scrutinize decisions and decision-makers. This includes journalists, academics and representatives of civil society. Governments may get involved by providing funding to support civil society in this regard, for example, and they may correct falsehoods related to their work. Such a system has served liberal democracies well for centuries, in theory at least. However, recent debates about fake news suggest that the system is no longer able to serve all members of society.

Information influence activities involve potentially harmful communication, but they are also something more. For one thing, they are conducted by foreign state actors or their representatives. This means that they are a form of deliberate interference in a country's affairs. Secondly, they are intended to support the interests of the foreign state. They interfere in a society, using deceptive communicative methods, to help achieve foreign policy goals. Thirdly, they are planned and targeted to exploit perceived vulnerabilities in a society. Foreign state actors study a society, its divisions, controversies and problems, and attempt to disrupt those areas of tension using illegitimate methods.

Such activities may be part of larger influence campaigns that draw upon a broad spectrum of techniques outside of the communication sphere to influence a society. In addition to information, means ranging from diplomatic, to economic and even military can be employed for this purpose.

ANATOMY OF AN INFORMATION INFLUENCE ACTIVITY

Makes use of influence techniques

Public relations, public affairs, public diplomacy and lobbying are examples of how organisations legitimately seek to influence public opinion in support of their interests by using a variety of communication techniques. Information influence activities mimic these forms of engagement but use the techniques deceptively.

Interferes in public debate

Foreign powers interfere in critical debates either directly or through intermediaries. This can include direct action, and indirect activities such as providing funding, manipulated documents, hacked materials, narratives, and amplification of messages. By interfering in public debate, they can distort the perception of public opinion and disrupt decision-making.

Have self-interested intentions

Influence activities are intended to achieve specific goals that benefit the foreign power. This can involve for example polarising political debate to hinder the agreement of policies that the foreign state wishes to avoid, or to destabilize a society in its entirety.

Exploits perceived vulnerabilities

All societies have problems. Some countries have social or class tensions. Others have geographic inequalities or problems with corruption. Hostile foreign powers identify key tensions in a society and systematically exploit those vulnerabilities to support their goals.

The ambiguity of these activities is a complex question which makes it hard to determine what is information influence and what is legitimate public opinion. Political debates can be sensitive, uncomfortable, and sometimes even distasteful. But they are part of a democratic process that relies upon openness and a variety of opinions. However, such debate cannot take place if hostile foreign powers feed deceptive information into that environment with the sole purpose of distorting the process of deliberation.

It is important to remember that having opinions similar to those of a foreign power does not make that person an agent of a foreign power. By information influence activities, we are talking about the systematic use of deceptive techniques that undermines democracy. Preserving free and open debate, democratic values, and our freedom of speech and expression should always be the cornerstone of our response to information influence activities, regardless of the challenges this may imply.

How are social vulnerabilities exploited?

Let's imagine that public opinion formation is a rational process. It begins with something happening somewhere, where a new piece of information comes to light. People who have credibility in that area will explain the event or information – be they officials, experts, scientists or witnesses. Media pick up this information and circulate it, and then it filters through communities who deliberate – online and offline – before it eventually reaches *you*. Obviously, opinion formation doesn't really work this way in practice, but in theory, ever since the Enlightenment, this is how philosophers and sociologists have spoken about how democratic societies *should* work.

This ideal process relies on some simple principles. It relies on the original event or information being genuine and supported by evidence. It expects claims to be verified by credible experts, officials or witnesses who are indeed real people with a reputation to lose if they distort the truth. Media should be balanced in their presentation, double-check facts and sources, and represent the public interest to some degree in their reporting. Deliberative communities are expected to weigh up 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. They can be opportunistic, creative and technologically advanced. They insert themselves into these steps to corrupt the circulation of information. They seek out vulnerabilities in how public opinion is formed, how media technologies circulate critical information, and even vulnerabilities in the ways our minds process information.

Evidence can be forged or manipulated. Experts can be brought in who aren't experts at all. Witnesses can be bribed or coerced. Media can be owned by state actors who use them as one-sided propaganda channels. Deliberation can be conducted between automated bots who give the impression of a lively public debate. When these activities are deliberately enacted, sometimes in coordinated campaigns aimed at undermining democratic processes, the system cannot always be expected to self-correct, at least not without a concerted response. This is where communicators come in.

Opinion formation

NEW INFORMATION

A new piece of information is added into the system; e.g. an event, a scientific breakthrough, a journalistic relvelation or a new political descision.

EXPERTS, OFFICIALS AND SOURCES

This new piece of 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.

PUBLIC SPHERE

Mediated messages enter a community. Here, individuals start talking about the information both through real life interactions and on social media platforms.

YOU

Finally, the information will reach you through the communities you are a part of.

MEDIA SYSTEM VULNERABILITIES

Our media system, in the context of rapidly changing technologies, changes in the journalistic business model, and a proliferation of citizen (ie unverified) news sources, is vulnerable to manipulation. From photoshopped letters & images, to fake experts on news channels, to social media clickbait, algorithms and bots, the media system is vulnerable to those who want to exploit it whether for political or economic gain, or even just to see if it can be done.

PUBLIC OPINION VULNERABILITIES

Public opinion formation has always been vulnerable to certain principles such as social proof – i.e. what somebody claims happened in their back yard. But together with social media accounts that are not what they appear to be and armies of trolls distorting comment fields, it seems easier than ever to provoke outrage and feed polarization, making public opinion formation vulnerable to deliberate manipulation.

COGNITIVE VULNERABILITIES

Some vulnerabilities are the result of how our brains are wired – we just aren't built to cope with many of the things we see and hear. Others, such as psychographic targeting, use our data to get to know us even better than we know ourselves. Some figures suggest that there can be as many as 800 data points on you that can be uzsed to predict almost everything about you. Information influence activities exploit how the human mind works to exert influence over individual perceptions, behaviour and decision-making.

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

It is not a communicator's role to investigate whether foreign powers are behind certain communications. You are expected to act when you suspect that information influence activities are being used in debates that are relevant to your work area, and where you have reasonable suspicion that these techniques are being used with the intention to undermine the integrity of public debate and undermine Sweden's national security. You are expected to use your judgment to make an assessment, nothing more. In other words, you need to have a basic understanding of your organisation's role in in the bigger picture, as one part of Sweden's democratic system and society.

To separate between information influence activities and other forms of legitimate communication, you need to assess the extent to which a piece of communication is deceptive, is intended to do harm and causes a disruption. By considering these factors when examining a case, you will be able to make an informed decision as to how to devise your response. It will not always be possible to ascertain the presence of all factors. However, the presence of increasing numbers of these factors will indicate the potential seriousness of an issue, and an increasing risk of information influence activities.

DECEPTION

Reliable communication is open and transparent about its source, origins and purpose. Its contents are credible and can be verified. Information influence activities are in contrast designed to deceive.

INTENTION

Reliable communication intends to contribute toward a constructive debate, even if the nature of the solution is contested. Information influence activities rather intends to undermine and limit constructive and open debate.

DISRUPTION

Reliable communication is a natural part of our society, even if it sometimes creates frictions, which strengthens our democracy. Information influence disrupts and weakens societal functions and democratic deliberation.

It is no coincidence that techniques employed in information influence activities often overlap with journalism, public affairs, public diplomacy, lobbying and public relations - mimicry of these techniques is part of the way in which information influence activities can appear legitimate. You should note, moreover, that illegal influence activities, such as threats, hacks, blackmail or 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 do these components fit together?

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 will develop a more nuanced understanding of the techniques that are used in information influence activities. We will help you to assess the main strategic narratives and audience targeting approaches that are used. We offer an overview of the main information influence techniques, and finally discuss how the strategies and techniques can be coordinated into combinations of techniques to produce negative social effects.

What is the purpose of information influence activities?

To identify information influence activities, you first need to be aware of two important dimensions that can reveal an overarching strategy, intention or purpose of an activity. These are strategic narratives and target groups. Basic awareness of these dimensions will help you better understand and identity suspected cases of information influence activities and give you some insight in the possible intention and purpose behind an activity.

Strategic narratives

Information influence activities usually involve storytelling of some kind. They may deliberately introduce falsehoods into stories about an event, issue, organisation, place or group of people. Often, what they want to say fits into a pre-existing debate or narrative. We will be familiar with these narratives because we use them unconsciously to sort new information. Everybody has heard the story of the space race, for example. It is also likely that many have heard rumours that the moon landings were faked. We sort new stories about space travel 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.

To offer an example, information influence activities involving disinformation about a specific religious or ethnic group will be designed to fit within broader historical and political narratives about that group. Disinformation is employed to suit this larger purpose. Sometimes, the logic will be to build a consistent narrative about that group. An alternative approach involves disproving established narratives to undermine that group. A third approach is to distract from the debate altogether if it isn't possible to influence it in other ways.

Identifying the strategic narratives at play and the logic of the communication techniques that engage with them is an important step in preparing counter measures. You should consider whether one or more of the following three approaches to strategic narratives are being used.

STRATEGIC NARRATIVES

Positive or constructive: "This is the truth!"
Tries to establish a coherent narrative or story about an issue. It fits within, 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 destroy an existing strategic narrative.

Oblique: "Look over here!"
Draws attention away from key issues, with the aim of distraction. Makes use of e.g. humour, memes, and conspiracy theories.

Target groups

Strategic narratives are one approach to identifying the logic of information influence activities. A second, connected approach is to consider for whom these strategic narratives resonate, that is, the target group. Are the narratives being targeted at everybody in a country, or just toward specific groups? 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 with what narratives is an important step in assessing the severity of the case.

TARGET GROUPS

General societal level: mass audiences
Information influence activities target society as a whole by aligning messages with narratives that are widely shared.

Sociodemographic targeting: specific groups
Used to identify audiences based on demographic factors such as age, income, education and ethnicity, allowing for more adaptation of messages.

Psychographic targeting: individuals
Big data is used to target individuals with specific personality traits, political preferences, patterns of behaviour, or other identifying features.

Analysing audience targeting can help to reveal the intention of the information influence activities. In conjunction with an analysis of the strategic narratives and communication techniques being used, an understanding of *who* is being targeted and *why* will allow you to make a reasonable assessment of *what* the purpose and goals of the information influence activities are. That will in turn help you to decide *which counter measures are most appropriate.*

What are the main information influence techniques?

Information influence activities continuously evolve. However, by studying a wide variety of examples, we have abstracted six common techniques that you should be on the lookout for. Within each group sub-techniques are characterised by similar principles. Awareness of how these techniques look and work will help you to recognise them.

In many cases, the techniques themselves are neither good nor bad – they are neutral. Communi-cation techniques can be used in open and accepted ways, or deceptively with hostile intent. The use of one of these techniques is not necessarily a sign of information influence. You should analyse the use of techniques in conjunction with your assessment of the deception, intention and disruption of the case, as well as your analysis of strategic narratives and target groups. Your analysis should always consider:

- How strong are the indicators of deceptive or disruptive intent?
- What do the strategic narratives and target audiences suggest about the purpose of the communications?
- If some of the main information influence techniques are being used, are they harmful to our population and/or society?

Information influence techniques

SOCIAL AND COGNITIVE HACKING

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

DECEPTIVE IDENTITIES

- Shilling
- Impersonators & impostors
- Forgeries
- Potemkin villages
- Fake media

TECHNICAL EXPLOITATION

- Bots
- Sockpuppets
- Deepfakes
- Phishing

DISINFORMATION

- Fabrication
- Manipulation
- Misappropriation
- Satire and parody

MALIGN 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 the ways that social relationships and thought-processes work. It is like hacking in the sense that hostile actors seek to cheat, or "hack", these processes. For example, we usually prefer to fit in with what people like us believe and do – it's part of having a group identity. Our minds take short cuts when they are exposed to, for example, emotional materials. These predictable patterns of behaviour can be exploited by hostile actors who deliberately activate trigger-points, for example in sensitive social debates.

DARK ADS

Messages are tailored based upon an individuals' psychographic profile. Big data can be used to create a database of individuals with a similar ideological stance and personality traits. Purchased advertisements that only they can see could include messages that appeal to their psychological leanings and encourage a certain form of behaviour or action.

BANDWAGON-EFFECT

People who feel like part of the majority are more likely to air their opinions. For example, bots can be used to boost the initial number of likes, comments and shares of a social media entry to facilitate further engagement from "real" users. This gives the impression of social acceptance, which appeals to the need for social conformity.

SPIRAL OF SILENCE

People who feel like part of the minority are less likely to air their opinions. In a similar scenario to the bandwagon-effect, the appearance of social conformity around an issue can cause people with contradictory opinions to remain silent. This appeals to fears of being excluded or singled-out because of an unpopular opinion.

ECHO CHAMBERS AND FILTER BUBBLES

Organically created sub-groups in which people only engage with others of similar opinions. Echo chambers exist both online and in real life. For example, voters for a political party may turn to the same newspaper for information, socialise predominately with peers from back-grounds like theirs, and engage in conversations on forums with people of a similar political orientation. Thus, they are rarely exposed to ideologically contradicting opinions. This can be exploited to reinforce and spread certain information to specific groups of people.

Deceptive identities

We often evaluate the credibility of information by looking at its source. Who is talking to me and why? What do they know about the issue? Are they who they claim to be? By imitating legitimate sources of information (be it persons, organisations or platforms), actors engaged in information influence activities exploit trust in the messenger by utilizing deceptive identities.

SHILLING

A shill is a person who gives the impression of being independent, but who is in reality working in partnership with somebody else. 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.

IMPERSONATORS & IMPOSTERS

Impersonators pretend that they are someone else, i.e. adopt someone else's personal or professional identity. Impostors do not pretend that they are someone else but pretend to possess expertise or credentials that they do not have, e.g. someone who falsely claims to be a medical doctor.

FORGERIES

Fabricating official documents is an effective way of making disinformation appear authentic. For example, fake letter heads, stamps or signatures can be used to produce forged documentation.

POTEMKIN VILLAGES

Actors with sufficient resources can set up institutions or even networks of institutions that serve to deceive and mislead. False companies, research institutions and think tanks are examples of so-called Potemkin villages which can create, and legitimate, false information.

FAKE MEDIA

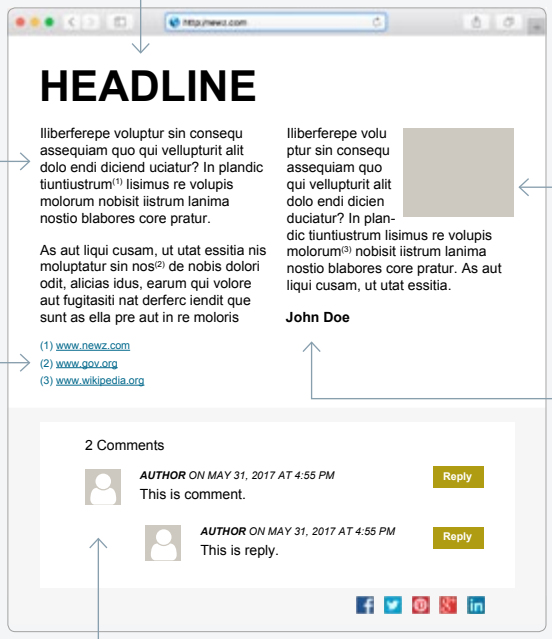
Disinformation can be circulated by creating fake media platforms that look like, or that have a web address similar to, a real news site.

Is the source genuine?

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

URL
Imitating well-known platforms to gain legitimacy is a known technique for information influence. 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 full text before sharing.



IMAGES
Images are not always a reflection of reality. They can be manipulated to add, remove or change a picture, or originate from a different context. It is possible to do an image search to find out if it has been used before.

SOURCES
If the text uses sources, make sure you follow the links to track the original statements. Assess whether it is used appropriately in the text.

AUTHOR
Be aware of texts without a by-line. If there is an author, consider who it is. Whether a text was written by journalist, a politician, an expert or a public citizen might provide some answers as to why it was written.

COMMENTS
Comments on webpages and in social media often look like everyday people expressing their opinions. But the accounts may also be controlled by trolls and bots spamming the platform.

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

Technical exploitation

Information influence activities often make use of, and exploit, new technologies. By using more advanced technical skills than most individuals possess, they can manipulate flows of information online. Manipulation can be conducted by individuals, by automated accounts or algorithms, and by combinations of people and automation. It should be noted that technical exploitation often uses a technological advantage to perform quite traditional information influence techniques such as deceptive identities, disinformation and forgery. Notably, the area of technical exploitation develops more quickly than our ability to analyse and understand its potential uses and consequences. Recently, issues associated with so called "deepfakes", machine learning and artificial intelligence (AI) have been highlighted in public debate, and we can expect that such tools will be increasingly utilised for information influence purposes in the future as well.

BOTS

Botar är datorprogram som utför automatiserade uppgifter, till exempel att dela vissa typer av information på sociala medier eller för att svara på vanliga frågor på en kundtjänstplattform. Inom informationspåverkan kan de användas till att förstärka utvalda budskap på nätet, spamma forum och kommentarsfält, gilla eller dela inlägg på sociala medier, eller för att genomföra cyberattacker.

SOCKPUPPETS

Imposter accounts managed by a person who does not reveal their real identity or intentions. These false identities are used to join online communities and participate in debates, and act as 'fronts' for introducing false or controversial information. Two or more sockpuppet accounts can be used in conjunction to simulate both sides of a debate.

DEEPFAKES

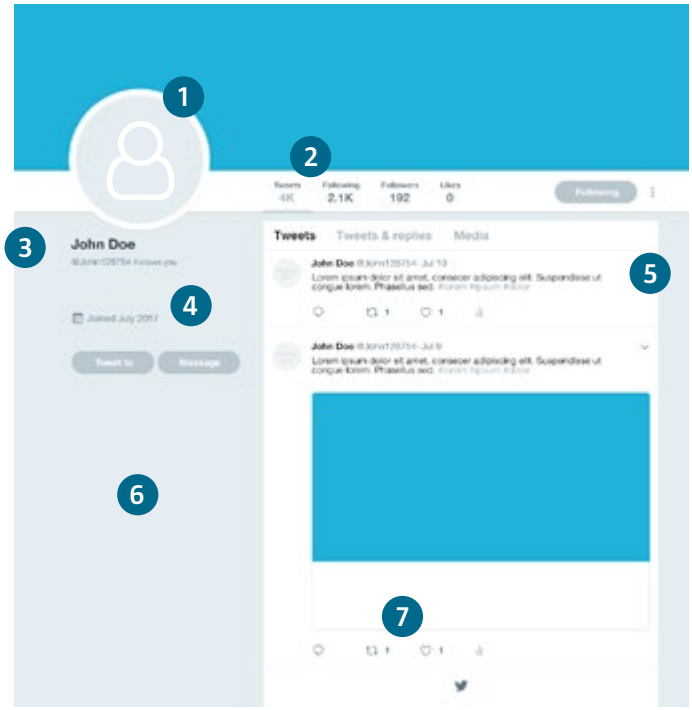
The use of learning algorithms to imitate voice and mouth movements for manipulating audio and video. This can for example be used to produce fake clips of a real politician delivering a faked speech. More advanced techniques can superimpose e.g. faces onto pre-existing video footage.

PHISHING

These approaches attempt to trick users into revealing passwords and other sensitive information. Phishing involves automated spamming of emails that look legitimate but that lead to fake websites which can then harvest any personal information entered. Spear phishing and whaling involve the more sophisticated targeting of individuals to gain access to e.g. their employer's secure computer system.

Spot the Bot

While bots are efficient tools of influence on social media, they are also vulnerable to exposure. The following seven steps will help you to spot a bot online. But be on your guard – different types of bots may look very different. Impersonator bots are designed to look like real users. Spammer 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. Google image searches can be used to validate profile pictures.

2 ACTIVITY

Spammer bots are often highly active, sometimes with more than 50 posts per day. Look out for accounts with a suspiciously high number of posts per day.

3 NAME

Most bots auto-generate their user names. Usernames at odds with the handle, or consisting of seemingly random letters and numbers are possible bots.

4 CREATION DATE

Bots are often young. Older bots will be re-purposed and hence old posts may have been removed. They may consequently have wide gaps between intense periods of activity.

5 LANGUAGE

Sometimes messages are automatically translated. This results in obvious grammatical errors or incoherent sentences. Accounts that publish in multiple languages may indicate a bot.

6 INFORMATION

Many bots exhibit a high degree of anonymity. Often this results in a display with little or no personal information.

7 ENGAGEMENT

Investigate which posts the account is engaging with. Bots often coordinate and amplify each other. They are likely to have few real followers.

Disinformation

Disinformation refers to inaccurate or manipulated information spread with an explicit intention to deceive and mislead its audience. It is the corner stone of classic propaganda, but it is also the basis of the more recent phenomena of fake news. The use of purposely false information for deceptive purposes is nothing new. However, digital platforms have fundamentally changed the way disinformation operates. Flawed content may consist of various manipulated elements such as text, image, video and audio. Disinformation 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 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

Ridicule, exposure and critique of individuals, narratives or opinions using humour and exaggeration. Though often harmless, this can be used aggressively within the framework of broader disinformation efforts. Humour is also very effective for legitimising controversial opinions.

Malign 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 malign rhetoric is not. Malign rhetoric exploits the often-fragmented nature of conversations in the contemporary public sphere to muddy the waters, deceive and mislead, and discourage actors and voices to participate in the public debate.

A common vehicle for online malign rhetoric is trolls. A troll is a user of a social media account who deliberately antagonises other users through their comments and behaviour. This contributes to increased polarization, silences dissenting opinions, and drowns out legitimate discussion. The troll is governed either by personal motivations or, as in the case of *hybrid trolls*, operates under the direction of someone else.

AD HOMINEM

Attacking, discrediting and ridiculing the person behind an argument to silence, deter or discourage.

WHATABOUTISM

Deflecting an argument by drawing attention to a similar phenomenon which does not get as much attention.

GISH-GALLOP

Overwhelming an opponent with a flood of arguments, facts and sources, many of which are spurious or unrelated to the issue.

STRAWMAN

Discredit an adversary by attributing positions or arguments that they do not hold and then arguing against those positions.

HIJACKING

Contributing to an existing debate by taking it over and changing the purpose or topic. Particularly effective when applied to hashtags, memes, events or counter-cultural social movements.

Symbolic actions

Actions speak louder than words. Sometimes actions are calculated to signal something, rather than to achieve the objective of the action itself. When this is the case, the action is a symbolic action. In contrast to any ordinary action, symbolic actions are motivated by a communicative logic and a strategic setting. This can be done very crudely, for by example playing on universally shared fears of random violence such as in terrorist activities. It can also be conducted in a sophisticated manner by relating to precise cultural symbols relevant only to a specific target audience.

LEAKING

Leaking consists of releasing information that has been obtained by illegitimate means. It carries symbolic weight as it traditionally reveals injustices and cover-ups not meant for the public eye. As an information influence activity, leaking often removes documents from their context and can be used to delegitimize actors and distort the information environment. Leaked information is sometimes obtained through hacking of IT-systems or theft.

HACKNING

Hacking means to gain unauthorized access to a computer or a network and is a crime. In information influence activities, hacking can serve as a symbolic action, by communicating that an organisation's data can be compromised, that a platform lacks security, or to open for blackmail.

PUBLIC DEMONSTRATIONS

Legitimate demonstrations are symbolic actions used to promote a certain political issue or position. Hostile actors can, however, exploit demonstrations to falsely give the impression of strong support or dislike of an issue (astroturfing).

How do these components fit together?

When identifying an information influence, you will need to weigh up strategic narratives, target audiences, and the communication techniques being used. When making your assessment, it is worth considering that hostile actors will rarely use one technique in isolation. Illegitimate communication techniques are often deployed as combinations of activities that support and reinforce one another.

For example, a forged document will get more extensive reach if it is spread by bots. If this can be coordinated with articles published on biased or fake news platforms and a troll army of commenters, the results can be more widely amplified. Your assessment should therefore consider whether there is any evidence of multiple, coordinated actions against you. On the following page, we offer some examples of what these combinations of activities might look like.

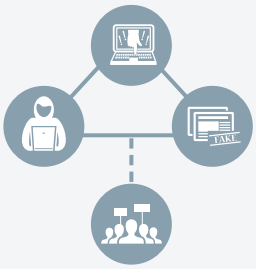
In identifying information influence activities, we have suggested that your assessment consider several factors. What are the stories and who are they aimed at? Is there any evidence of an intention to deceive or disrupt? Do you suspect interference in the debate from a foreign actor or their proxies (both conscious and unwitting)? Is there a combination of techniques that is suggestive of a concerted effort or campaign against you? If your assessment leads you to be concerned about the issue, you will find several suggestions for counter-influence techniques in part III.

Combinations of techniques

Information influence operations can be complex, and you will rarely encounter one technique in isolation. You should look out for when a combination of techniques is being used against you. While the possible combinations are theoretically infinite, it is worth noting some common combinations.

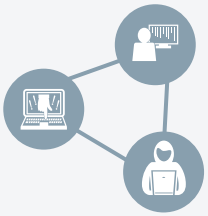
Polarisation

Polarisation supports two opposing extremes of a specific issue. This is achieved by supporting pre-existing perspectives, using social hacking, deceptive identities online, and disinformation. Often trolls and bots are used to further a polarised discussion.



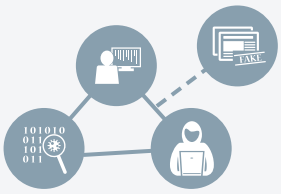
Laundering

Laundering refers to gradually distorting and de-contextualizing information, so that it becomes impossible to tell if its source is true or false. Here, deceptive identities, disinformation, technical manipulation and symbolic action combine with social and cognitive hacking to create a web of false information.



Enraging

Enraging takes advantage of sensitive issues in public debate. This combination utilizes social and cognitive hacking, deceptive identities and malign rhetoric to engage ordinary citizens by invoking their emotional relationship to a specific issue.



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.

PART III: Countering information influence

How do I prepare my organisation?
How do I choose an appropriate response?
How do I make sure that lessons are learned?

PART III: Countering information influence

In this section, we will discuss approaches to counteracting information influence activities. We will help you prepare your organisation to meet this threat, discuss what action to take 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
Fact checking
Social media

LEARN

Describe
Reflect
Share

How do I prepare my organisation?

Preparation is the most essential part of any type of contingency or crisis management plan. It allows for quick and efficient responses by establishing the right mindset and structures. Preparation consists of a number of stages. First is raising awareness, both by contributing to your organisation's awareness and to broader society's knowledge of these issues. Second is to develop messaging, narratives, and an understanding of how your key audiences and stakeholders may be vulnerable to certain kinds of information influence activities. Third is risk and vulnerability analyses for your organisation.

Raise awareness

The first step toward dealing with a problem is admitting that the problem exists. A main component of preparedness is raising awareness of the threats and vulnerabilities that we as a society, and you in your organisation, face. On a societal level, the best defence against information influence activities is to develop the capacity to handle threats. This means creating cross-sector platforms where leaders, governments, journalists and media representatives, social media platforms, researchers and communication professionals can exchange knowledge and best practice with each other and with the general public.

As a communication professional in a public-sector organisation, there are also things you can do to help build capacity within your organisation. Firstly, you will be a key point of contact for these issues within your organisation. In particular, you will need to talk about these issues with senior management, and in internal communication with your colleagues. Secondly, you should perform a coaching role for your leadership and colleagues so that they are aware of what to do if faced with information influence activities. This includes identifying training needs and opportunities. Thirdly, you will need to liaise with colleagues outside of your organisation and build relationships based on mutual support and exchange of experiences.

Build trust through strategic communication

One of the goals of information influence is to undermine trust between people and societal institutions. Therefore, the effect of these activities can be minimised by focusing upon counteractivities that establish trust in public institutions. Managing the reputation and legitimacy of public institutions is an important aspect of any counter measure strategy.

Prepare messaging & narratives

Since it may take time to gain clearance for messaging during times of crisis, it is important to prepare generic messages that assert your organisation's values, and that can be readily adapted to a specific occurrence. Just as organisations use messaging to explain a new initiative or product, it can also be used to raise the awareness of fake stories and for debunking them.

PREPARED MESSAGES

Quick responses on social media are made possible by prepared, pre-cleared messaging. For example, the Metropolitan Police in London sent its first tweet just seven minutes after the Westminster terrorist attack of March 2017. It gave accurate information about the unfolding situation but was based upon a generic message prepared for similar scenarios.

When designing messaging, it is important to consider the stories that circulate about an organisation, that create the broader narratives. The narratives will be connected to audience perceptions. You should consider how individual messages contribute to the identity, values and narratives that your organisation wishes to project, particularly in relation to different audiences. Messaging that supports positive narratives about your organisation can play a crucial role in shaping resilience to falsehoods.

WHAT'S YOUR STORY?

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

A strong narrative derives from a clear sense of organisational identify, values and goals.

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

Attacks on narratives should be countered by upholding those values that the organisation stands for.

Know your public

Establishing your core values, messaging and preferred narratives is closely connected to an understanding of which public and stakeholder groups are most vulnerable to influence, or most important for you to reach in case of a sudden crisis. You will already possess expert knowledge of how to conduct target audience analysis. The difference here is that the analysis is centred upon which audiences are most vulnerable to deceptive and disruptive influence, and why. You should try to identify which parts of society are most likely to be the target of information influence activities and consider what kinds of messaging they are susceptible to. Once you have done this, you can prepare suggestions for how these audience members can be reached with counter- or preventative messaging.

TARGET AUDIENCE ANALYSIS

Audiences and public groups do not simply exist

Publics are "produced" by their common views, beliefs and interests, through their relationship to an organisation, an issue or in their relationship with each other. It is important to understand which factors unite members of a target audience.

Create stakeholder maps

Information influence activities related to your organisation does not only damage you. It is vulnerable members of society who can be most affected. It is important to know which groups may be most at risk by assessing their relationship to you and their vulnerability to certain narratives.

Map your core narratives

Identify narratives that can be used to respond to information influence, by linking them to target audiences. Include possible intermediaries with high credibility for those groups.

The goal of these exercises is to prepare communication assets that can be used if information influence activities are used against you. They are a form of crisis contingency planning adapted to situations where illegitimate communicative methods are used to falsely undermine your reputation. The goal is to restore trust as quickly and efficiently as possible. These assets include the preparation of messages and narratives that are targeted to segments of your audience. It includes preparatory work for understanding how different audiences, and particularly stakeholders, can be affected by disinformation, and which messaging is appropriate to them.

Know your organisational risks and vulnerabilities

In addition to the above, organisations should prepare a formal assessment of how information influence activities can threaten their ability to function. Risk and vulnerability analysis is already part of your organisation's strategic planning. It's therefore suggested that information influence activities are added to existing risk and vulnerability analyses, with a specific focus upon vulnerable stakeholders/audiences, key values, messages and narratives, and the overall risk to core organisational functions.

RISK AND VULNERABILITY ANALYSIS

Step 1: Point of departure

What is your organisation's role and responsibilities?
Which methods will be applied to identify and assess threats?
What delimitations and perspectives will be applied in the analysis?

Step 2: Risk assessment

What are the possible threats and risks?
What is the probability of these risk, and what are the possible consequences?
Which scenarios should be evaluated in relation to the organisation's crisis management abilities?
What preventative actions should be taken?

Step 3: Vulnerability assessment

How will different scenarios affect the organisation?
What would the consequences of information influence activities be, and how can the organisation manage, resist and recover from it?

Step 4: Risk management

What should be done if information influence activities are identified? See following sections for examples.

How do I choose an appropriate response?

There is no one-size-fits-all response to information influence activities. As we have established throughout this handbook, the activities vary greatly. More importantly, your organisation will have different vulnerabilities than others. Your preparatory work will help to clarify these challenges. It is also important to consider that each public-sector organisation has different expectations placed upon its communicators. Deciding on an appropriate response is closely tied to your role, the expectations placed upon you, and the mandate you are given by your organisation's leadership to respond.

Assess, inform, advocate or defend?

In determining an active response, it is worth considering what kinds of response may be considered proportionate to the threat. We suggest four categories of response, that each consist of several specific communicative techniques. We suggest examples of techniques belonging to each category on the following page.

The first level of response is to assess the situation. This is a neutral response that signals that you are aware of the issue and are ascertaining the facts. The second level seeks to inform the public and key stakeholders of your position. This is a slightly less neutral response that outlines what you consider to be the facts of the case. Both categories are broadly applicable: that is to say, they can be used in most if not all cases without risking controversy or criticism. They are the building blocks of a rational, fact-based response which can be used in any situation.

The third level of response involves communications 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 defend. In this case, you will take a specific response against your attacker. These levels are the building blocks of an advocacy-based response. While they may be appropriate depending on the severity of the situation they should always be used with caution.

Fact-based responses

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

Suggested examples of the kinds of responses that you could use within each approach.

STEP 1: ASSESS

To know what you are dealing with you need to make an assessment of the situation. What is really going on? Who is involved? What is at stake? The better situational awareness you can create for yourself, the better your response will be.

MAP THE SITUATION

Orient yourself to the situation you are dealing with to create a firm situational awareness. Use the tools highlighted in Part I & II to determine what you are dealing with.

FACT CHECK

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

NOTIFY STAKEHOLDERS

Be it colleagues or external stakeholders, the sooner you can inform them of what is going on, the better.

INVESTIGATE TRANSPARENTLY

Engage reliable external actors, such as journalists, in investigating the issue to ensure transparency.

ISSUE A HOLDING STATEMENT

Communicate that you are looking into the issue by issuing a holding statement, giving you time to develop a more thorough response.

STEP 2: INFORM

Once you have an idea of the situation, you can progress to inform your audiences of what you consider to be the facts of the case and how you are dealing with the situation. Remember to utilise target audience analyses when designing your messages.

MAKE A STATEMENT

Lay out the facts of the case as you see them.

CORRECT

Make a statement that directly responds to false allegations with facts, or that debunks a piece of disinformation. A Q&A can be a useful tool for this.

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.

Advocacy-based

The second and third levels are advocate and defend. They are appropriate in more clear-cut and severe situations and make up an advocacy-based response.

Suggested examples of the kinds of responses that you could use within each approach.

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

Actively engage in a dialogue with key stakeholders and members of the public.

FACILITATION

Make sure information is easily available to your target audience. Organize events or meetings that bring different stakeholders together to discuss a specific problem to help your audiences to make sense of your position.

MULTIPLIERS

Engage with key actors who act as gatekeepers for important stakeholder groups to amplify your message.

PIGGYBACKING

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

DÉMARCHE

Prepare a dossier on the issue that will help you present your case, using multiple sources of evidence.

STORYTELLING

Relate the situation to a broader narrative about, for example, your organisation and its values through advocacy-based storytelling which will help your target audience understand the situation.

STEP 4: DEFEND

Defending involves designing a direct response against your attacker. This step can appear controversial and should therefore be reserved for extreme cases. Make sure to discuss your planned line of action with colleagues and leadership first, to avoid exceeding your mandate or contributing to worsening the situation.

IGNORE

Sometimes the best response is to do nothing. This might be suitable if the case gains marginal attention or where your response might provide legitimacy to the case.

REPORT

If the attacker breaks the law or a platform's code of conduct it may be necessary to report them to the police or the owner of the platform. This should not be done lightly. Reporting users to the owner of the platform should never be abused or done without care - this should only be done for clear violations, to avoid silencing public debate.

BLOCK

Communicators should be acutely aware of the need to respect freedom of speech and refer to the appropriate governing code of conduct before blocking a user. Yet, clearly disruptive activities may merit blocking from a specific platform. Each blocking should, however, be clearly motivated on the basis of the code of conduct on the platform. Blocking should never occur for the sake of avoiding a tough argument or dodging an inconvenient user.

EXPOSE

Although not recommended, a strategic response to information influence activities could include exposing the actor behind, for example, an illegitimate or false account. Again, this should not be done lightly. If you consider exposure as your response, make sure to conduct a proper consequence analysis beforehand which considers the consequences an exposure could have for your own organisation, your stakeholders, and the person who is exposed.

The choice of which categories of response to use should be weighed up against your assessment of the severity of the situation. Information influence activities with weak indicators are best met with rational, fact-based responses. Aggressive information influence activities may require a fact-based response in conjunction with a more assertive defence utilising advocacy techniques. If you decide to use the latter two categories, we urge caution. If they are to be used, you should make sure that you have the mandate from your leadership to do so, and ensure that the 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

An important aspect of the two first levels of approaches (assess & inform) is that your communi-cation is, at its core, neutral and fact-based. Assessing and informing should always be the first fact-based response. If an advocacy-based response is also used, it builds upon facts as a first, compulsory layer. If inaccurate information is allowed to circulate without correction, this can contribute to perceptions of you, your organisation or parts of your key audiences based on falsehoods.

The process of fact checking involves understanding how falsehoods affect your organisation's work. The first step is to consider those stories about your organisation that are relevant for fact checking. The assessment can be based on various aspects, such as who said it, how widely it is spread, or what the story is about. Public organisations may for example look for stories featuring quotes from the organisation's representatives, viral stories within the community, or claims about the organisation and the field in which it operates. To assemble a fact-based point of departure for the assessment of the story either as true or false, the following approach is suggested.

Assessment

- ☑ Collect non-partisan expert opinions and/or accurate data from relevant sources.
- ☑ Request more information from the person or organisation making the claim.
- ☑ Search for the original source of the false data.

If the story is adjudged to be false, a corrective response will be an appropriate step. Many experts agree that disinformation is best counteracted by accurate information. However, some argue that you will only reach those pre-disposed to finding out the truth. Your preparatory work on audiences and narratives should give you an advantage when assessing how and when to respond.

Developing a fact-based response See also: The Debunking Handbook (2012)

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

If you have the ability and mandate to launch a persuasive advocacy-based response, such a response should be based on the lines established in a fact-based response.

Special considerations for social media

Social media are not just platforms where users can easily engage with each other. They are also important forums where information influence take place. The medium has its own logic, which should be harnessed in counter influence activities. It is difficult to be sure of who is behind a social media account, from where their information is sourced, and whether their network represents a contingent of genuine public opinion. It is also a challenging medium as it requires a quick response where one need not only consider the message itself, but elements such as *tagging, name calls, linking,* and *attached files*. A typical social media post will contain one or more of these elements, which together contribute to positioning the post within a network of accounts, ideas and debates.

TAGGING

Creating a search term for an item. Tags often define the circulation and reach of a post.

NAME CALLS

Tagging a person or organisation's account so that they are notified of a post.

LINKING

Providing a hyperlink to a different part of the internet. Links are often shortened, hiding the URL of the site.

ATTACHING FILES

Multimedia files such as an image or video. Note that they can change the meaning or intention of a post.

Proactive social media work includes building networks and establishing hashtags that enable an organisation to get messages out to the right people. 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 listen for potential threats or vulnerabilities to their reputations in real time. It is therefore an advocacy tool for dialogue and messaging, and an open source intelligence tool for understanding important trends.

Counter responses for social media

The four levels of counter response provide a general approach to counter-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 combined knowledge of information influence. Is it a case of information influence activities or just concerned citizens engaging in debate? If you think it is likely to be illegitimate influence, map the situation as clearly as possible. Which users are engaging with you? Are they antagonists themselves or reacting to something that an antagonist has prepared? Which hashtags are used? Are there 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 your conclusions of your assessment. Carefully select which users, hashtags and audiences to engage with. Focus on clarifying your position and assert your organisation's values using your established 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 multimedia or pre-prepared messages. At this stage it may also be appropriate to involve yourself more in the debate and engage users directly. You can also utilize your following to promote engagement for your cause.

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!

How do I make sure that lessons are learned?

Collecting and documenting examples of information influence activities is crucial to furthering our understanding of the problem. Furthermore, examples of your responses, and assessments of whether the responses achieved their desired effect, is essential to establishing best practice. That knowledge can be used to develop training material and to improve preparation within your organisation and in society more widely. Such information should be shared with communicators in similar roles, with public authorities tasked with identifying information influence activities (e.g. in Sweden, MSB), and in some cases, with the public.

The following page gives some examples of the kinds of information that you should save if you have dealt with a case of suspected information influence:

Learning

DESCRIBE

- [x] Describe the case context and background.
- [x] What where the actors and networks involved? (avoid speculation if you don't know).
- [x] To what extent did the case meet the definition of information influence activities?
- [x] What was the nature of the vulnerability exploited?
- [x] What influence techniques were used? Include activity chains and narratives.
- [x] Does the case fit within a broader pattern of activities?

REFLECT

- [x] What do you think where the intended effects? Describe the evidence to support this claim.
- [x] How did you act? Reflect upon the order and logic of these steps
- [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 lessons do you take from this example?

SHARE

- [x] Have you saved evidence or data related to the case?
- [x] Are you discussing information influence activities with your organisation's leadership and colleagues?
- [x] Do you have regular contact with colleagues working on similar issues in organisations similar to yours?
- [x] Are you actively sharing your expertise and experience with others inside and outside of your organisation by participating in training and events?

Strategic considerations

Countermeasures are limited by the fact that they respond to somebody else's agenda. In this regard, the entire principle of countering information influence activities has a premise that is problematic, since the aggressor may appear to be setting the conditions under which a nation's democracy can or cannot properly function. It feels like they *act* and we *respond*, and that we are destined to remain a step behind the latest attempts to exploit vulnerabilities in society's systems.

It makes more sense to focus on upholding democratic values, which depend upon open debate and free speech. Your job is to protect the process of opinion formation as it relates to your organisation by minimising the effects of vulnerabilities in the media system, public opinion, and cognition. We recommend a robust but measured fact-based response.

It is worth reiterating that efforts to counter information influence activities should never have the effect of silencing public debate. This will only lead to further polarization and a breakdown of societal functions and defeat the purpose of what you are trying to do! Open and democratic debate must always be protected and encouraged. We recommend an approach based upon:

- ☑ Raise the threshold for information influence activities through raising awareness and preparing
- ☑ Developing proactive, proportionate and sensible communicative responses that place the audience (rather than the adversary) in focus and upholds shared societal values
- ☑ Upholding a face-based response that can be developed into an advocacy-based response under specific circumstances
- ☑ Sharing best practice and learning from one another
- ☑ Be vigilant but not paranoid!

Further reading

This handbook is based on the following report:

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

You can find the report along with a full reference list on MSB's website:

https://www.msb.se

We recommend reading the report if you wish to deepen your understanding of information influence activities. 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 Foundation 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

Swedish Civil Contingencies Agency (MSB)
SE-651 81 Karlstad Phone +46 (0)771-240 240 www.msb.se/en
Order No. MSB1263 - July 2018 ISBN 978-91-7383-867-2