RESIST model: a quick guide

Recognise disinformation

What are the objectives of disinformation?

What are the techniques of disinformation?

How does disinformation combine techniques to achieve an impact?

Situational insight

What is insight in the context of disinformation and how should it be used to support a timely response to disinformation?

Strategic communication

What should a public response to disinformation look like?

What is the sign-off process?

What are the available options for responding?

R E S I S T

Early warning

How do I focus digital monitoring on my priorities?

How do I build a digital monitoring toolbox?

How can I use digital monitoring to assess potential threats and vulnerabilities?

Impact analysis

What is the likely goal of the disinformation?

What is the likely impact of the disinformation?

What is the likely reach of the disinformation?

How should I prioritise the disinformation?

Track outcomes

How should I record and share information about the disinformation campaign?

How can I evaluate my actions and understand the lessons learned?

Recognise disinformation

Disinformation is about **influence**. The people who spread it do not want members of the public to make informed, reasonable choices. They try to achieve a goal by deliberately shortcutting normal decision-making processes. The basic techniques are simple – we call them the **FIRST principles of disinformation:**

- **Fabrication** manipulates content: for example, a forged document or Photoshopped image;
- **Identity** disguises or falsely ascribes a source: for example, a fake social media account or an imposter;
- **Rhetoric** makes use of malign or false arguments: for example, trolls agitating commenters on a chat forum;
- **Symbolism** exploits events for their communicative value: for example terrorist attacks; and
- **Technology** exploits a technological advantage: for example bots automatically amplifying messages.

These FIRST principles of disinformation are often **combined to create an impact.**

FIRST principles, combined

1. Look for a social issue that is sensitive or holds symbolic value.
2. Create two or more social media accounts under false identities.
3. Manipulate content to provoke a response within the sensitive issue.
4. Release the content through one account, then criticise it through others.
5. Use bots to amplify the manipulated content to opposing networks.
6. Use memes and trolling to give the impression of a heated public debate.

Potential impact:
Undermine confidence in government or between social groups; contribute to political polarisation; earn money through clicks; go viral and reach mainstream news.

Early warning

You will need to do some preparatory work to better understand exactly **what** you want to monitor. The answers to the below questions will help you to **focus** your digital monitoring on the issues that matter most for disinformation. This step can be used in different stages and kinds of planning.

	Priorities	Attitudes
Policy objectives	What are my **priority policy areas** and objectives?	What are the prevailing attitudes in these areas that could be harnessed for disinformation?
Influencers	Who are the **key influencers** affecting my policy areas?	What are their prevailing attitudes toward my organisation or our objectives that could be harnessed for disinformation?
Audiences	Who are my **key audiences?**	What are their prevailing attitudes toward my organisation or our objectives that could be harnessed for disinformation?

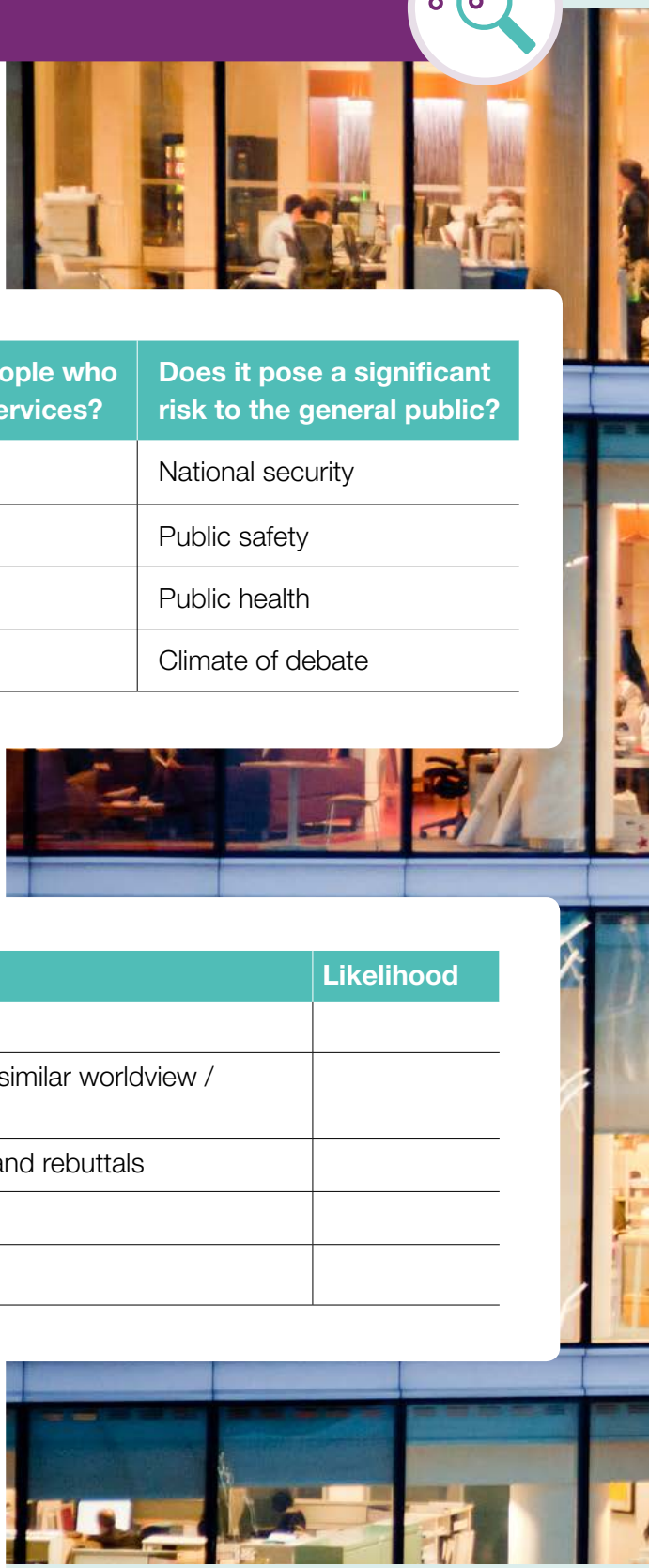
This work can help to guide your digital media monitoring so that you are prepared to identify any indicators of potential threats at the earliest possible stage.

Situational insight

Monitoring becomes valuable when it is turned into **insight**. Insight is a form of analysis that turns **interesting data** into **actionable data**. It answers the question, 'so what?' At its core, insight is about understanding audiences to support communication planning. A disinformation insight product should at a minimum include:

- key insights and takeouts: a top line summary including a short commentary explaining the 'so what' and setting out your recommendations for action; and
- sections on key themes and issues covering:
  - relevant outputs from your department on priority issues, for example a ministerial announcement;
  - examples of disinformation relating to these outputs, including where and how it is circulating;
  - key interactions and engagements;
  - trends and changes in attitudes over time (this can be combined with any polling data you have); and
  - your commentary and recommendations for a response.

Impact analysis



If you have identified some disinformation that relates to your organisation, you should make an assessment of its goals, impact and reach. This is achieved by answering a number of questions which can guide you in deciding whether to respond. For example, you should ask:

Does it affect the ability of your organisation to do its job?	Does it affect the people who depend upon your services?	Does it pose a significant risk to the general public?
Ability to deliver services	Key stakeholders	National security
Reputation	Key audiences	Public safety
Policy areas/goals	Niche audiences	Public health
Individual staff/staff safety	Vulnerable audiences	Climate of debate

You should make an assessment of how extensively you believe the disinformation will be engaged with. Is it likely to disappear within a few hours or does it have the potential to become tomorrow's headlines?

Exposure/reach	Likelihood
Little interest: very limited circulation and engagement	
Filter bubble: some engagement within niche audiences with similar worldview / automated circulation	
Trending: some discussion online, may include open debate and rebuttals	
Minor story: some reporting on mainstream media	
Headline story: affecting day-to-day operations	

Once the previous steps are completed, you should be able to assign a priority level to the disinformation. Is the disinformation likely to become part of a major cross-governmental crisis, like the Skripal poisoning? Or is it enough simply to monitor developments? The principle is that the goal, impact and reach should inform how urgently you prioritise the case.

	Description	Actions	Audiences	Tools
High	The disinformation has the potential to affect national security and has a high likelihood of making headlines. It requires immediate attention and escalation.	Make senior staff, SpAds / policy advisers and other parts of government aware of the issue and its priority. Share insight and analysis. Prepare quickly for a cross-Whitehall response.	- Senior staff - Wider government	- Share insight - Briefings - Prioritise short-term communications
Medium	The disinformation has the potential to negatively affect a policy area, departmental reputation or a large stakeholder group and is trending online. It requires a response.	Make senior staff and SpAds / policy advisers aware of the issue. Share insight and analysis within department. Investigate the issue and prepare press lines based on known facts.	- Senior staff - Policy advisers	- Insight - Briefings - Press lines - Prioritise short and medium-term communications
Low	The disinformation has the potential to affect the climate of debate and has limited circulation. The debate should be routinely followed but intervention is unnecessary/ undesirable.	Share insight and analysis within media department. Investigate the issue and prepare press lines/narratives based on known facts. Conduct a baseline analysis of debate and track any changes.	- Comms officers	- Insight - Press lines - Baseline analysis - Prioritise medium and long-term communications

Strategic communication

You can now consider a range of communicative approaches, such as short-term/reactive options, medium-term/proactive options, and long-term/strategic options.

You can combine them into a tailored communication strategy aligned with the OASIS communications planning model. For example, your response could include:

	Action	Target groups	Tools
Short-term reactive	The disinformation requires an immediate response. Use rapid communications to rebut, correct or counter disinformation in accordance with the established facts.	- Traditional media (journalists/editors) - Stakeholders and influencers - Social media platforms - Key audiences	- Press statement - Minister statement - Brief journalists - Q&A - Paid advertisement - Search engine optimisation (SEO) - Expose actors via friendly influencers

	Action	Target groups	Tools
Medium-term proactive	The disinformation requires a considered response. Use a combination of communications to assert own values/brands. Tie together proactive measures with your normal everyday communications and work with stakeholders/influencers to create consensus around your position.	- Traditional media (journalists/editors) - Stakeholders and influencers - Social media platforms - Wide audiences	- Campaign, narrative and brand development - Community outreach, dialogue and engagement - Facilitate network, stakeholders and influencers - Workshops/training

	Action	Target groups	Tools
Long-term strategic	The disinformation requires a coherent, sustained response to create long-term change. Develop and assert strategic narratives in relation to an issue by shaping the information space to promote your own position and deter others (raising the threshold).	- Traditional media (journalists/editors) - Young up-and-comers - Stakeholders and influencers - Social media platforms - Wide audiences	- Campaign, narrative and brand engagement - Programme funding e.g. for participatory content - Talent spotting and influencer support/ creation - Facilitate network, stakeholders and influencers - Workshops/training - Contingency planning

Track outcomes

You can evaluate your decision-making and actions based on the above steps, using a common format that enables you to share lessons learned.

Recognise disinformation: provide a bottom-line overview of the disinformation techniques used, including visual examples.

- What was the goal of the disinformation?
- What disinformation techniques were used?
- How were the disinformation techniques combined to achieve an impact?

Situational insight: once you have identified disinformation, consider how well your initial analysis and situational briefing supported your team's response.

- Were we able to offer an accurate and timely briefing to colleagues?
- Did we make any incorrect assumptions? On what basis?

Strategic communication: provide an overview of the communicative responses you took broken down into actions, target groups and tools.

Early warning: consider your preparatory work and the extent to which it supported your efforts to handle disinformation.

- Is your digital monitoring sufficiently focused on your priorities?

Impact analysis: consider your assessment of the likely goals, impact and reach of the disinformation.

- Was the disinformation prioritised correctly, based on goals, impact and reach?

Track outcomes: collect this information in a dossier together with your assessments of the actions you took.

- What was the impact of your efforts to handle the disinformation?
- What lessons can be learned from this case?