EU vs Disinfo

GUIDE FOR PUBLIC COMMUNICATORS ON PRO-KREMLIN DISINFORMATION

UNDERSTAND – RECOGNISE – RESPOND

INTRODUCTION

Over the last decade, developments in digital and communication technology have radically transformed the way we produce, consume, and share information. On the one hand, making it easier to produce and disseminate information creates important opportunities for voices that would ordinarily be left out of the public debate. But at the same time, as witnessed over the last few years, these same tools can be exploited and abused to undermine democratic societies. Authoritarian states and other malicious actors have weaponised these tools to spread disinformation and manipulate democratic processes around the world.

Disinformation is a very complex challenge, spread and coordinated by multiple state and non-state actors and their proxies, taking advantage of the digital revolution through multiple channels and in many languages. Four years of work on the EUvsDisinfo project, carried out under the umbrella of the European External Action Service, has led us to conclude that Russia is leading the race to pollute the public debate. With one of the most far-reaching and large-scale disinformation campaign against Western values and institutions, the Kremlin is endeavouring to manipulate and undermine democratic processes in the European Union and its Member States.

Other actors, both within the EU and outside of it, are using manipulation techniques, disinformation narratives, and behavioural tactics straight out of the Kremlin's playbook. The disinformation challenge is now not only multifaceted but also ubiquitous, concerning everybody who has so much as an internet connection, a TV, or a smartphone. It is becoming increasingly difficult to move freely in the information space without being targeted by disinformation. In many cases, it is difficult even to recognise disinformation or identify its source, let alone react to it in a constructive manner.

To better tackle this challenge, the EU adopted an Action Plan against Disinformation in December 2018, which also serves as the backdrop for this handbook. In line with the title, its aim is to guide public communicators through the peculiarities and intricacies of disinformation. It starts by outlining the basic principles, aims, techniques, and narratives of disinformation in order to help even ordinary citizens understand and recognise this phenomenon and the challenges behind it. The second part of the guide situates disinformation in the context and discipline of strategic communications. It provides hands-on tools and recommendations about how to respond effectively should your organisation or institution be targeted by a disinformation campaign. In preparing these recommendations, we reviewed best practices also proposed by others, namely the handbook for communicators by the Swedish Civil Contingencies Agency[1] and the Counter-Disinformation Toolkit by the UK's Government Communication Service[2], both of which are must-reads for public communicators.

Finally, the guide includes a brief compilation of the most common pro-Kremlin disinformation narratives, together with evidence-based counterarguments, to help you respond effectively if and when you are confronted with such claims.

We hope that this guide will be a useful reference for people dealing with communications not only professionally but in their everyday life.

EUvsDisinfo Team
East Stratcom Task Force
European External Action Service
www.euvsdisinfo.eu
STRATCOM-EAST@eeas.europa.eu

LIST OF CONTENTS

PART 1.

DISINFORMATION –

WHAT IT IS ABOUT

Four years of monitoring, analysing, and exposing pro-Kremlin disinformation through the EUvsDisinfo project – from the continuing subversion of Ukraine to interference in numerous elections around the world – leave little doubt that no country has weaponised digital disinformation on a global scale more successfully than Russia.

Today, there are many actors pursuing disinformation and digital manipulation tactics to achieve their aims. Nevertheless, an extensive body of evidence collected by researchers, public institutions, and other organisations conclusively documents the Kremlin's interference in online debates and electoral processes in Europe and across the Atlantic Ocean, whether in online discussions about Brexit, the annexation of Crimea, or the presidential elections in France in 2017 and the US in 2016.[3]

Since 2014, the Kremlin has pursued a single primary objective: to weaken the West and strengthen Russia in a classic zero-sum game approach. Despite the diversity of messages, channels, tools, ambitions and tactical aims behind the Kremlin's disinformation operations, this strategic objective remains constant. Operating in over 100 countries, with billions of dollars

behind this operation, the pro-Kremlin disinformation machine tailors its narratives to reach the most vulnerable audiences[4].

For the Kremlin, disinformation is a non-military measure for achieving political goals. Russian authorities are explicit about this: the Russian Minister of Defence has stated that information is "another component of the armed forces"[5], while top generals consider "false data" and "destabilising propaganda" as legitimate tools. The leadership of Russian state-owned media also subscribe to this view: the editor-in-chief of RT (Russia Today), one of the most notorious pro-Kremlin outlets that is active all around the world, has said that the network serves the same role as Russia's Defence Ministry[6].

The Kremlin has turned to disinformation as a cost-effective and scalable strategy to undermine the West from within, weaponising core democratic values like free speech, press freedom, and unrestricted access to information. The goal is to fuel widespread social fragmentation and mistrust, undermine democratic institutions, damage trust between allies, and ultimately paralyse the West's ability to act in its self-interest and to defend its values.

In practice, disinformation can take various forms and serve different strategic purposes. It can be both offensive and defensive: for example, used as a tool of electoral interference against another country, or to justify acts of Russian aggression, like the annexation of Crimea. At the same time, the Kremlin's disinformation playbook is also highly predictable. It seeks to relativize the very concepts of truth and fact by polluting the information space with misleading and contradictory information. The ultimate aim is to alter the target's perception of reality and lead them to act in ways that benefit their opponent. And other actors, both within the EU and outside, use the same tactics.

FOUR D's OF PRO-KREMLIN DISINFORMATION [7]

DISMISS THE CRITIC

DENY ALLEGATIONS AND ATTACK THE CRITIC

DISTORT THE FACTS

TWIST INFORMATION OR OMIT CRUCIAL BITS OF CONTEXT TO SERVE THE DESIRED AGENDA

DISTRACT FROM THE MAIN ISSUE

DEFLECT NEGATIVE ATTENTION BY LAUNCHING CONSPIRACY THEORIES OR ACCUSATIONS AGAINST OTHERS

DISMAY THE AUDIENCE

DEMORALISE AND INTIMIDATE THE OPPONENT USING THREATS AND FEARMONGERING

PART 2.
HOW TO RECOGNISE
DISINFORMATION

Disinformation tactics are often deployed as part of a broader influence campaign. To identify them, it is first necessary to understand the strategic aims and narratives of this campaign. This chapter provides practical tools and tips for identifying the warning signs of disinformation.

Recognising disinformation is not always easy. Often it can be just a single sentence in an article that supports an overall strategic narrative.

CAN YOU FIND DISINFORMATION IN THIS ARTICLE?
'MIGRANT FREE' SLOVAKIA IS IN TOP THREE OF SAFEST EU COUNTRIES

The safest countries in the European Union are in order: Croatia, with only 3 per cent of Croatians reporting crime, violence or vandalism in 2017. Poland, having only 5.4 per cent and third, again, Slovakia, with 6.2 per cent.

Slovakia has accepted very few refugees or migrants during the European migrant crisis and has no problems concerning terror, no-go zones or sex crimes.

The EU average is 11.6 per cent, CTK newswire reports, with Bulgaria bottoming out the list with 23.6 per cent of Bulgarians reporting crime, violence or vandalism. As high as that is, it has actually been dropping over the past three years since it peaked at a record 28.6 per cent in 2009.

"The 'Peace, Justice and Strong Institutions' survey focuses on progress made in ensuring peace and personal security, in promoting access to justice and increasing trust in EU institutions," the Eurostat website explains.

By **LAURA CAT** — 4 December 2018

Prime Minister of Slovakia, Peter Pellegrini - photocosmos1 / Shutterstock.com

The full analysis of this case is available here:
https://euvsdisinfo.eu/report/more-migrants-more-crime-and-less-safety-in-the-eu/

IN FACT:

This article repeats the common pro-Kremlin narrative that migrants are a threat to the EU and the security of its Member States. The original Eurostat data[8] to which this article refers does not make any link between public safety and the presence of immigrants (or lack thereof). Moreover, according to the same data, the country with the highest rate of reported crime, violence or vandalism is Bulgaria - a country that has among the lowest number of migrants.[9] The statistical information in the article was manipulated to suggest a non-existent correlation between the size of a country's migrant population and the safety of that country.

SO, HOW CAN WE RECOGNISE DISINFORMATION? HERE'S A CHECKLIST:

1. TAKE A CLOSE LOOK AT THE SOURCES

When you encounter a suspicious article or social media post, first check the source and author.

QUESTIONS TO ASK:

➡ **What are the most frequent topics addressed by the author, the website, or the media outlet?**

> 💡 *TIP :*
> *If the content frequently exploits one or more of the pro-Kremlin narratives, there is a high possibility that disinformation tactics are also being used.*

➡ **Is it a reliable and trustworthy source of information?**

> 💡 *TIP :*
> *Run the author and/or the article through a fact-checking website. Has it been mentioned there? Disinformation is likely to be repeated by a source that has been identified by fact checkers.*

➡ **Does the photo seem suspicious?** Use Google Reverse Image[10] search or a similar tool to verify its authenticity. It could have been taken in another location and falsely attributed to the article.

According to the title and date of this article, the image is attributed to Kosovar and Albanian migrants in 2018. In fact, the image is from 2016, from the border between FYROM (now North Macedonia) and Greece. It shows migrants and refugees, mainly from Syria.

The origin of this image was determined using Google Reverse Image search.

The full analysis of this case is available here: https://euvsdisinfo.eu/ one-image-4-x-disinformation-about-migrants

➡ **Is this case new or recycled?** Disinformation is often recycled. Articles from years ago sometimes resurface in their original form, and in some cases are adjusted and revised with new elements. If you see a suspicious article that looks similar to something you have seen or heard before, search for it online and look for references.
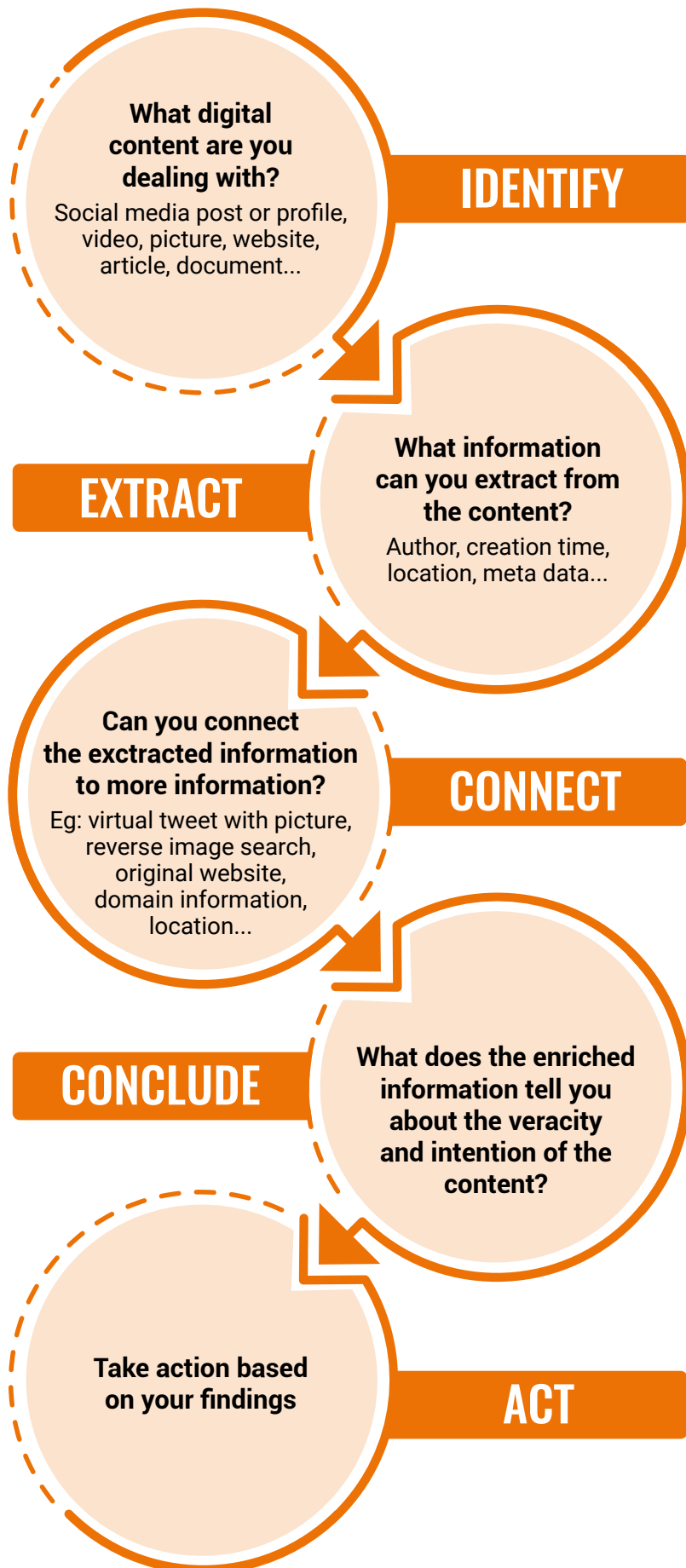
➡ **Have you considered using one of these tools to identify disinformation?**
Have fact checkers addressed the article or story? Check against these sources:
  ➡ European Commission: Euromyths
  ➡ European Parliament Think Tank: Disinformation
  ➡ Bellingcat
  ➡ DFR Lab
  ➡ IFCN Code of Principles
  ➡ Polygraph
  ➡ EUvsDisinfo

If you need more information, check out EUvsDisinfo's list of resources: https://euvsdisinfo.eu/reading-list/

IDENTIFY

What digital content are you dealing with?
Social media post or profile, video, picture, website, article, document...

EXTRACT

What information can you extract from the content?
Author, creation time, location, meta data...

CONNECT

Can you connect the exctracted information to more information?
Eg: virtual tweet with picture, reverse image search, original website, domain information, location...

CONCLUDE

What does the enriched information tell you about the veracity and intention of the content?

ACT

Take action based on your findings

There are many tools to collect, analyse, and verify digital content. The key is to know which ones to use, when to use them, and where to find them.

The art of online investigation is:
a) extract information from digital content (a social media post or profile, video, image or website), and
b) link and contextualise it with more information.

It is best to start your analysis by learning as much as possible about a piece of content. If information is available but hidden, use tools to make it visible and then further research it.

It is hard to keep up with all the analytical tools available. Fortunately, there are curated lists of useful tools and techniques:

GUIDES

➡ **RESIST: Counter-Disinformation Toolkit**
The UK government's counter-disinformation toolkit to help communications professionals counter the threat posed by disinformation;
https://gcs.civilservice.gov.uk/guidance/resist-counter-disinformation-toolkit/

➡ **Countering information influence activities**
A handbook for communicators by the Swedish Civil Contingencies Agency;
https://www.msb.se/RibData/Filer/pdf/28698.pdf

TECHNIQUES

➡ **Webbreacher's "OSINT Graphical Analyzer" YOGA**
An open-source project and visualisation that helps to answer the question: *I have this information. What can I transform it into or use it for?;*
https://webbreacher.com/2018/06/24/introducing-osint-yoga/

➡ **OSINT map**
A multi-tabbed mind map where each tab provides a guide through an OSINT process and engagement;
https://webbreacher.com/2018/07/12/osint-map/

TOOLS

➡ **Bellingcat's Online Investigation Toolkit**
Bellingcat's list includes satellite and mapping services, tools for verifying photos and videos, websites to archive web pages, and much more;
https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit

➡ **OSINT Framework I - Bruno Mortier**
A directory and collection of tools and sources;
https://start.me/p/ZME8nR/osint

➡ **OSINT Framework II - Justin Nordine**
A directory and collection of tools and sources – but with a network interface;
https://osintframework.com/

➡ **OSINT Framework III - Aware Online**
A number of OSINT scripts written by The Aware Online Academy that allow you to search for online information;
https://www.aware-online.com/en/osint-tools/

➡ **Learn all the things**
A collection of OSINT frameworks, contains many of the lists above, but also links to communities of researchers;
https://www.learnallthethings.net/osint-resources

2. WATCH OUT FOR THE MOST COMMON DISINFORMATION NARRATIVES...

As research shows,[11] pro-Kremlin disinformation is most often based on thematic narratives that are tailored to different contexts, topics, and audiences according to the Kremlin's specific needs. Being familiar with the most common narratives is another effective way to recognise disinformation coming from different sources, not only from the Kremlin and its proxies.

THE ELITES VS. THE PEOPLE

This narrative is based on the populist trope that "evil elites" are out of touch with ordinary people. It is often used in conjunction with conspiracy theories that target groups like Jews, corporations, globalists, climate activists, and EU bureaucrats, among many others. The objective of this narrative is to fuel grievances and drive wedges into the target society, pitting different groups against each other to undermine civic cohesion. In some cases, this narrative is used to delegitimise elections by suggesting that they have been manipulated by certain powerful groups.

⚑ WATCH OUT FOR THESE RED FLAGS

No evidence:

Claims are not supported by any evidence, but presented as unquestionable truth

Scapegoating:

A group of people is indiscriminately vilified as evil, immoral, or corrupt and blamed for a particular grievance, whether real or invented

THREATENED VALUES

This narrative is adapted to a wide range of topics and is typically used to challenge progressive Western attitudes about the rights of women, ethnic and religious minorities, and LGBTQI groups, among others. Values-based disinformation usually centres on concepts like "tradition", "decency", and "common sense" – terms that all have positive connotations but are rarely clearly defined. This narrative often suggests that traditional values are under threat from "progressives" who are seeking to impose a morally bankrupt dystopia a line that is often effective in eastern Europe. Russia, meanwhile, is portrayed as the righteous defender of the Christian moral tradition.

⚑ WATCH OUT FOR THESE RED FLAGS

Vague values-based language:

Terms like "tradition", "decency", "family values", and "morals" that are supposedly under threat in the West

Liberal decay:

Attacking liberal values, including minority, gender, and LGBTI rights, as morally degenerate

LOST SOVEREIGNTY

The premise of this narrative is that some countries no longer possess national sovereignty or independence, either because they are under someone else's control, or because they are being taken over by other corrupting forces (e.g., Islam, LGBTI groups, feminism, etc.). Accordingly, this narrative has a dual purpose: it can be used to stoke people's fear about their country's future, and it can be used to undermine trust between allies by insinuating that one country is "master" and the other its "vassal".

⚑ WATCH OUT FOR THESE RED FLAGS

External occupation:

A country is described as being occupied, a "vassal state", or ruled by someone else

Corruption of national identity:

Corrupting forces, usually of a liberal nature, pose an existential threat to national identity

IMMINENT COLLAPSE

This narrative is broadly directed at the Western institutional order and specific organisations like the EU and NATO. In some cases, it also takes aim at individual countries, for example suggesting that they are on the verge of civil war or that their economy is collapsing. The primary function of this narrative is fearmongering, particularly among vulnerable audiences who already fear political and social instability. This narrative is thus especially effective during periods of turmoil and crisis events, like the 2015 migration crisis or after terrorist attacks.

⚑ WATCH OUT FOR THESE RED FLAGS

Apocalyptic predictions:

Ominous and often vague warnings about impending war, collapse, or other disaster

3. … AND THE RHETORICAL DEVICES THAT ACCOMPANY THEM

In addition to these narratives, pro-Kremlin disinformation relies on a number of common rhetorical devices and deceptive arguments that serve the four D's agenda (see page 5).

WHATABOUTISM

Attempting to change the subject and discredit an opponent's position by accusing them of hypocrisy, usually without any evidence. The Kremlin regularly attempts to dismiss its critics by accusing them of the same offense (or worse), without actually addressing the criticism in question.

"The MH17 investigation unjustifiably accuses Russian citizens, but at the same time, there are no sanctions against Saudi Arabia for the journalist Jamal Khashoggi's murder''.

This particular example from the EUvsDisinfo database tries to marry two completely separate issues to divert attention from Russia's proven complicity in the shooting down of MH17.

The full case based on this article is available in the EUvsDisinfo database:
https://euvsdisinfo.eu/report/mh17-and-the-khashoggi-probe-where-are-the-sanctions-against-the-saudi-regime/

TRUTH IS SOMEWHERE IN THE MIDDLE

This tactic involves suggesting that truth is a matter of perspective and cannot be objectively determined. Often, this argument is used precisely in cases where truth *can* be determined using facts and evidence. For example, in cases like the downing of MH17 or the Skripal poisoning, the truth about who is responsible (Russia) is not a matter of perception. The facts are black and white.

HAHAGANDA

When confronted with compelling evidence or arguments, a last-resort reaction by pro-Kremlin media is to ridicule or make light of the subject. In connection with elections, for example, this involves the use of disparaging language to deride the concept of democracy, democratic procedures, and individual candidates. Kremlin aide Vladislav Surkov describes the concept of democracy as "a battle of bastards" and instead recommends the "enlightened rule" of Vladimir Putin as an alternative for Europe.

As another example, RT (Russia Today) sought to trivialise and ridicule the Salisbury attack by presenting a chocolate replica of the Salisbury Cathedral as a gift to Russian channel TV Rain, which is critical of the Kremlin.

Source: TV Rain via BBC.[12]

"TRUST ME, I'M AN EXPERT!"

Facts are not dependent on a narrator's intelligence or education. Unfounded claims are still unfounded, no matter how clever their claimant appears to be. Sometimes the "experts" who appear in pro-Kremlin media don't have any track record in the field they claim expertise in. In other instances, they specialize in everything, from foreign policy to the Deep State to ancient aliens.

KREMLIN WHITEWASHERS

It's not a sin to be sympathetic to the Kremlin. However, the problem arises when Russia's or the Kremlin's bad behaviour is justified or excused at all costs, typically by blaming the West for alienating Russia and destroying the relationship. For example: "Russia's aggression is simply a response to Western neoimperialism and the expansion of NATO!"

Check out the annex of this guide to find more examples of such narratives.

ACCUSIONS OF FASCISM

Russia's frequent invocations of fascism are the consequence of the national mythologisation of the unique role of the Soviet army in the victory over Nazi Germany in World War II. Russia is still fighting that war to keep its own glory alive, and sees mythical fascists everywhere. Countries that often fall victim to these types of attacks are Ukraine and the Baltic States, among others.

CONSPIRACY THEORIES

Conspiracy theories are a common tactic common tactic aimed at audiences interested in theories about the Deep State/the Establishment/the Corporations/the Jews/the Gay Lobby/somebody or something else ruling this world. These often go hand in hand with the "Elites vs. the People" narrative described above. Conspiracy theories are by definition unfalsifiable, because they incorporate evidence that speaks against them, and thus become a matter of faith rather than fact. You don't want to go down that rabbit hole!

THE GLOBAL OFFENSIVE OF CORRUPTING MORALS AND DESTROYING VALUES

10.10.2019

One example of a conspiracy theory from the EUvsDisinfo database is using Alfred Kinsey, the scholar who challenged conventional beliefs about sexuality in the 1940s and 1950s in the US, to ''showcase'' the West's decadence and immorality. The full analysis of this case, based on the article shown above, is available in the EUvsDisinfo database: https://euvsdisinfo.eu/report/alfred-kinseys-1948-report-on-sexuality-was-designed-to-promote-the-most-deviant-sexual-behaviors/

4. DON'T BE PLAYED

Disinformation often targets emotions, appealing to our sense of injustice, fear, urgency, disgust and other negative feelings. Images, emojis, and strong headings add to the emotional message of the article or social media post. Pay attention to how they are used in combination to convey a particular message.

QUESTIONS TO ASK:

➡ **Is the headline shocking and/or emotional?**
➡ **Does the text in the article support the heading?**
➡ **Check the photo** – what message is the author trying to convey with it?

💡 *TIP :*
Take a look at this study by the Eindhoven University of Technology about seven things that make disinformation appealing: https://euvsdisinfo.eu/7-factors-which-make-disinformation-appealing-to-our-brain/

5. LOOK OUT FOR GRAMMAR AND SYNTAX MISTAKES

Disinformation can come from other countries and might be distributed by individuals who don't speak the language with native proficiency.

💡 *TIP :*
Some languages, like Russian, do not use articles. If the suspicious post is in English, look for the use of definite and indefinite articles ("the" and "a"). Are they frequently added where they do not belong or omitted where they are necessary? Also examine sentence structure. If texts read strangely in a systematic way, this can also be a clue that a non-native speaker is pretending to be somebody else.

6. CONSULT THE WEBSITE'S CONTENTS

Sometimes disinformation is distributed by websites and/or social media accounts that were created temporarily just for this purpose. Look out for these clues to spot inauthentic websites or accounts.

QUESTIONS TO ASK:

Take a look at this example:

➡ **What is the website's internet address?** What extension (the last part of web address after ".") does it have?

> 💡 *TIP :*
> *Be wary of the web addresses of known media outlets or organisations that seem different than usual – for example, with extensions like *.info. This could be a fake website created to imitate a trusted source.*

➡ **Does the website provide author names?** Check them online – what information can you find about them?

> 💡 *TIP :*
> *Sometimes disinformation is linked to authors that do not exist. The authors might also be real, but their background might suggest that they don't have expertise on the topic they are writing about. See EUvsDisinfo's analysis about fake authors on one particular website: https://euvsdisinfo.eu/the-journalists-who-exist-only-on-paper/*

➡ **Check the "About" section.** Does the website have a physical address? Is there an organisation behind it?

> 💡 *TIP :*
> *Check the physical address of the website in through a search engine.*

WHY WOULD A CENTRE BASED IN HELSINKI HAVE A *.RU EXTENSION?

When the fake website was created in 2017 to target the Hybrid Centre of Excellence in Helsinki, it looked very similar to the real website, which had (and still has) this domain: https://www.hybridcoe.fi

Read more about copycat websites: https://euvsdisinfo.eu/a-fake-fact-checker-again/

➡ **Does the website link to other websites to support its articles?**

> 💡 *TIP :*
> *Take a look at EUvsDisinfo's story about the website called "EP Today", which almost exclusively reposts articles from a limited number of sources, including RT (Russia Today): https://euvsdisinfo.eu/how-to-get-the-european-parliament-to-read-russia-today/*

7. BECOME A BOT AND TROLL SPOTTER

Disinformation on social media is often distributed by bots and trolls. Bots are computer programmes that perform automated tasks. Trolls are real internet users who usually hide behind fake profiles. Trolls and bots often work together to support each other in the spread of disinformation.

QUESTIONS TO ASK:

➡ **Does the account have a profile picture?** Bots often lack it, whereas trolls might use a stolen one. Search for the picture online to verify its origin!

➡ **What's the account's name?** Bots can generate their names randomly. Trolls can take a fake name – search for it online to see if that person exists.

➡ **When was the account created?** Bot and troll accounts are usually created for a specific purpose. Check the date when they were created – the content of the messages could be linked to the date when the accounts were created (elections, summits, anniversaries of historical events, major political events – wars, protests, etc.).

➡ **How active are they?** Bots are very active on social media. Sometimes they generate tens or hundreds of posts posts a day. Trolls are often occupied with only sharing links to other websites.

> 💡 *TIP :*
> *Free tools like Twitonomy [13] collect many available tweets from one Twitter account and reveal more about a profile's activities, interests and connections. Use it to check the activity of a suspicious Twitter account.*

➡ **Does the language sound ok?** Bots sometimes use automated translation. Trolls might make grammar mistakes that are atypical for the kind user they want to impersonate. [14]

> 💡 *TIP :*
> *If you see a suspicious social media post that has unusual engagement patterns, check what users are engaging with it. Are they real humans or bots? Bots are often used to create the impression of high engagement on a particular post; that gives a signal to the social media algorithms to make the post more visible.*

At the other end of the spectrum are accounts that share a lot of links to pro-Kremlin sources but lack any engagement, i.e., reactions that they would normally get from a genuine circle of friends. Such accounts work as amplifiers, increasing the number of times a specific article has been shared, and can be repurposed to troll others by posting insulting or nonsensical comments.
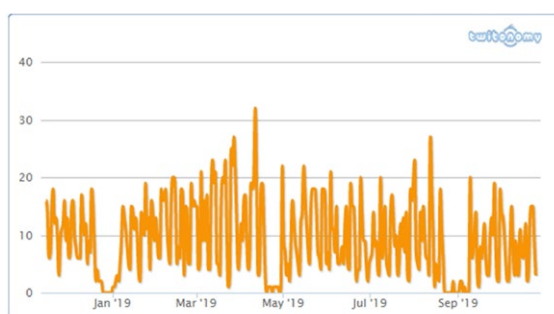
> 💡 *TIP :*
> *It is seldom possible to say with 100 percent certainty that a given account is part of part of a coordinated Russian troll operation. [15]*

HERE'S AN EXAMPLE OF THE AVERAGE ACTIVITY OF HUMAN-OPERATED AND AUTOMATED ACCOUNTS:
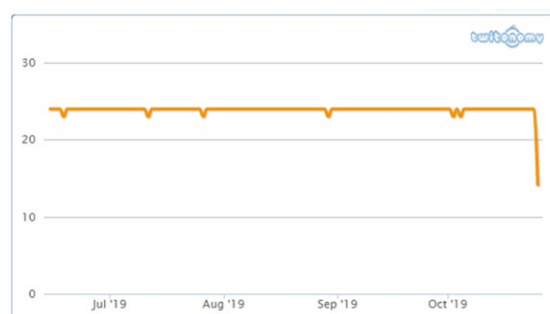
"NORMAL" ACCOUNT

➡ **Activity per day of a human controlled account:**

AUTOMATED ACCOUNT

➡ **Activity per day of a bot account:**

PART 3:
HOW TO RESPOND
EFFECTIVELY

Disinformation can target your organisation as a whole or employees individually. Follow these steps to determine the best response.

STEP 1.
THINK AND COMMUNICATE STRATEGICALLY

Disinformation tactics use vulnerabilities, including gaps in the communication of your organisation. Prepare and plan your communication activities strategically to explain the policies of your organisation and choose topics for pro-active communication to build your reputation. Developing a communication strategy together with an activity plan will help.

ELEMENTS TO INCLUDE
IN THE COMMUNICATION STRATEGY:

➡ **Objectives.** What are the main objectives of the overall communication of your organisation in the longer term (over 1-2 years)?

> 💡 *TIP :*
> *Keep the number of objectives low*
> *(i.e. 1-3 key objectives) and more general.*

➡ **Target audiences.** What are the main target audiences for your objectives?

> 💡 *TIP :*
> *"General population" is often included in*
> *communication strategies as the main target*
> *audience. Try to be more precise & realistic*
> *when defining your target audience.*

➜ **Messages.** What are the main messages that would effectively explain the objectives to the target audience?

> 💡 *TIP :*
> *The more relevant the message is to the target audience, the more effective it will be.*

➜ **Tactics.** What channels should be used to reach the target audience? What is the best format to distribute the messages?

> 💡 *TIP :*
> *Think about the available budget when deciding on tactics and adjust your tactics to be realistically supported by your budget.*

➜ Evaluation. Did your communication support the objectives? Did your messages reach the target audiences? Did you use your communication budget effectively?

> 💡 *TIP :*
> *Consider carrying out public opinion surveys to test the progress on achieving your communication objectives. Social media platforms provide analytics about views and engagement on your social media posts.*

OBJECTIVES
WHY?

TARGET AUDIENCE
WHO?

MESSAGES
WHAT TO SAY?

ACTIVITY PLAN
HOW?
WHEN?
HOW MUCH?

EVALUATION
IMPACT?

STEP 2.
PREPARE

Disinformation is often repeated; it refers to strategic narratives and myths and it uses the vulnerabilities of your organisation. Take your time and prepare arguments to respond to myths about your organisation.

STEP 3.
IDENTIFY AND ASSESS

When faced with a disinformation claim, it is important to assess it, closely monitor it and gather information to decide on the best response. Here are questions to consider:

➡ **What is the actual disinformation claim?**
➡ **What is its source?**
➡ **Is it a one-off case?** Or do you notice this case being distributed via more channels?
➡ **What is the social media engagement for this case?** Who are the people commenting on it?
➡ **How many people has the disinformation message reached?** What is the risk of it reaching wider audiences?

> 💡 *TIP :*
> *Disinformation is often distributed in a coordinated manner across different channels. If you notice that the same disinformation story is shared via different actors and channels (i.e. social media, websites) in the same timeframe, it is important to respond quickly to reduce the risk of disinformation entering the mainstream media.*

STEP 4.
CONSIDER YOUR RESPONSE OPTIONS

There is no one-size-fits-all response to disinformation, and the decision on the way to respond is always difficult. On the one hand, responding to a claim with limited impact could add visibility to it. On the other hand, ignoring a disinformation claim could allow it to spread further and have a larger impact.

OPTION 1: IGNORE

If this is a limited disinformation case without a large impact and is unlikely to receive widespread attention, you may choose to ignore it.

> 💡 *TIP :*
> *If you decide to ignore the disinformation claim, it is important to continue monitoring this claim in order to respond to it if it starts gaining attention.*

OPTION 2: RESPOND WITH FACTS

If you notice that the disinformation claim is gaining attention, consider issuing a factual statement, identifying the disinformation claim, providing a factual correction and describing steps you have taken to address it (i.e. contacting the outlet that distributed the claim). You can also use the statement to remind the audience about the values your organisation stands for. Distribute this statement to media and to your stakeholders.

> 💡 *TIP :*
> *An official statement will help media to identify the disinformation and not fall victim to it by multiplying it. Important: when issuing the statement, do not link to the actual disinformation claim, so that you don't contribute to its spreading.*

ANNEX:
THE WORLD ACCORDING TO
PRO-KREMLIN DISINFORMATION

Now that you know the objectives and tactics of pro-Kremlin disinformation, and you know how to become more resilient against them, check out the most common disinformation narratives. As you can see below, they come in different shapes and sizes, but the core of the narrative remains the same.

We also provide you with fact-based arguments to respond to them, to assist you if you come across these narratives and decide to react to them.

NARRATIVE 1.
THE WEST IS RUSSOPHOBIC
AND SO ARE RUSSIA'S NEIGHBOURS

Whenever the Kremlin's policies abroad are criticised or met with a response, the pro-Kremlin media turn to the narrative of so-called "Russophobia".

"Russophobia" is used to explain everything: EU sanctions against Russia; the investigation of the downing of Malaysia Airlines Flight MH17; international reactions to the poisoning of Sergei Skripal, and much more.

The Kremlin is always innocent, and Russia is always the victim.

IN FACT:
➡ EU sanctions against Russia were imposed as a response to the illegal annexation of Crimea and the violation of Ukraine's territorial integrity.
➡ A special international investigation has conclusively shown that Flight MH17 was shot down by a Russian missile system. The EU has called on Russia to accept its responsibility and to fully cooperate with all efforts to establish accountability.
➡ British police and intelligence services have produced hard forensic evidence that was sufficient to charge two Russian nationals for the attack on the Skripals.

Within a year of the Skripal poisoning, EUvsDisinfo compiled 151 different pro-Kremlin narratives about the incident.

NARRATIVE 2.
THE WEST IS AGGRESSIVE AND CLOSING IN ON RUSSIA

In the world of the pro-Kremlin disinformation, Russia is surrounded by enemies: NATO has expanded to threaten Russia, while the West aims to undermine Russia and is preparing for an attack or maybe even WW3.

With this narrative, the pro-Kremlin media keeps its audiences in perpetual fear. If Russia is surrounded by enemies, then all of the Kremlin's policies are justified.

IN FACT:
➡ NATO seeks no confrontation and poses no threat to Russia. Since the 1990s, NATO has consistently sought to build a partnership with Russia.
➡ No other NATO partner had been offered more comprehensive avenues for cooperation. They were limited only after Russia illegally annexed Crimea and started an armed aggression against Ukraine.
➡ The Baltic States and Poland chose to join NATO and the EU, in line with their sovereign right.
➡ The EU and NATO respect Russia's sovereignty. At the same time, they encourage Russia's further democratisation and support civil society, promote human rights and freedoms within the limits of the law.

> *Poland and the Baltic States are often portrayed not only as aggressive, but also neo-fascist. Such narratives facilitate historic revisionism and denial of Soviet crimes and occupation.*

NARRATIVE 3.
EUROPE IS WEAK, IN DECAY AND MORALLY CORRUPT

In the eyes of pro-Kremlin disinformation, Europe is a highly dangerous place, morally corrupt, balancing on the verge of decay. The migration crisis is presented as an "Islamisation" of Europe, pitting criminal migrants against hapless local populations. The EU's support for equal rights to minorities is misconstrued as a proof of existential dangers to national and individual identities. The EU itself is presented as suffering under the yoke of political correctness and simultaneously aiming to impose its dictate of human rights, gender equality and non-discrimination on its neighbours.

This allows the disinformation campaign to portray Russia as a defender of traditional values against the wave of alternative views of the world. Russia owns moral superiority, and the Kremlin is presented as a guardian.

IN FACT:
➡ The EU's advocacy for the rights of the LGBTI persons, ethnic and national minorities and gender equality is based on the principle of equal rights and dignity for all human beings.
➡ According to the Pew Research Centre, the proportion of Muslims in Europe will rise from 6% to 8% between 2010 and 2030.

> *There is no line the pro-Kremlin media will not cross to illustrate the Europe's alleged moral corruption. Sexual deviance and crimes, human and organ trafficking, even Satanism – Europe has been accused of it all.*

NARRATIVE 4.
EUROPEAN COUNTRIES HAVE LOST THEIR SOVEREIGNTY; GENUINE GRASSROOTS MOVEMENTS, CIVIL AND POLITICAL ACTIVISM DO NOT EXIST

Pro-Kremlin disinformation outlets often claim that certain countries are no longer truly sovereign. Examples of this narrative are numerous: Ukraine is presented as ruled by foreigners. Europe is allegedly ruled by the US. Germany is still occupied. NATO and the EU are pursuing militaristic and bureaucratic ambitions, disregarding the interests of their member states and citizens.

Political and civil protests in Russia's neighbourhood and especially in Russia never reflect genuine discontent of the people, but rather the wishes of some "overseas masters".

IN FACT:
➡ European integration does not imply the surrender of national sovereignty. Countries join the EU at their sovereign will. European treaties ratified by national legislatures regulate which policies are decided on the national level and which at the European level.
➡ NATO maintains an open-door policy to enlargement; however, the process starts only after a country expresses its aspiration to join and upholds certain democratic, economic and military standards.
➡ Transatlantic and international cooperation in the fields of security, economy and other areas is a normal practice of international relations; it does not mean a loss of sovereignty.
➡ The EU has never staged, nor does it intend to stage a colour revolution in Russia or any other country. The EU continues to support civil society and human rights defenders around the world, including in Russia.

The EUvsDisinfo database shows that pro-Kremlin media recycle specific keywords related to the colour revolutions. Watch out for "Russophobia", "puppet/puppet master", "provocation" and "deep state", and the

West (especially US) staging colour revolutions in post-Soviet states; the "Arab Spring" revolts; Ukraine's Euromaidan in 2014; protests in Hong Kong; protests in Moscow; protests in Georgia; and the Yellow vests protests.

NARRATIVE 5.
UKRAINE: A FAILED AND AGGRESSIVE STATE

Ukraine remains the primary target of pro-Kremlin disinformation. Pro-Kremlin disinformation targeting Ukraine is an extension of hybrid warfare against Ukraine's sovereignty.

Ukraine is routinely portrayed as verging on political and economic collapse, a haven for neo-fascists that implements ruthless policies of discrimination against the country's Russian speakers.

The pro-Kremlin media continues to legitimise the illegal annexation of Crimea with claims of a "democratic referendum". Russia's armed aggression in the east of Ukraine is presented as a Ukrainian civil war, and the Maidan popular uprising in 2014 as a *coup d'état*.

IN FACT:
➡ There is no civil war in Ukraine. Ukrainian sovereignty and territorial integrity has been violated by the acts of aggression of the Russian armed forces since February 2014.
➡ No international body has recognised the so-called referendum in Crimea. The Office of the Prosecutor of the International Criminal Court has stated that the situation in Crimea amounts to an international armed conflict between Ukraine and the Russian Federation.
➡ There was no coup d'état in Ukraine. In 2013, Ukrainians protested against the decision of Ukraine's former president not to sign the EU-Ukraine Association Agreement. Subsequently, Ukraine held democratic presidential elections on 25 May 2014.
➡ Ukraine is a democratic state undergoing a complex reform process with support of the EU and other international partners.

4 out of 10 disinformation cases compiled in the EUvsDisinfo database are about Ukraine.

ENDNOTES

(¹) https://www.msb.se/RibData/Filer/pdf/28698.pdf
(²) https://gcs.civilservice.gov.uk/guidance/resist-counter-disinformation-toolkit/
(³) To consult the research and its sources, see: https://euvsdisinfo.eu/european-elections-2019/
     and https://euvsdisinfo.eu/reading-list/
(⁴) For more information about the Kremlin's disinformation tactics, see EUvsDisinfo analysis:
     https://euvsdisinfo.eu/the-strategy-and-tactics-of-the-pro-kremlin-disinformation-campaign/
(⁵) http://www.interfax.com/newsinf.asp?id=581851
(⁶) https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88
(⁷) This term was coined by Ben Nimmo, for more information about the concept, see:
     https://www.youtube.com/watch?v=yIsh9kGLMwM
(⁸) https://ec.europa.eu/eurostat/web/products-eurostat-news/-/WDN-20181127-1
(⁹) https://ec.europa.eu/eurostat/statistics-explained/index.php/Migration_and_migrant_population_statistics
(¹⁰) https://www.google.com/imghp?hl=en
(¹¹) https://euvsdisinfo.eu/the-strategy-and-tactics-of-the-pro-kremlin-disinformation-campaign/
(¹²) https://www.bbc.com/news/uk-england-wiltshire-46699507
(¹³) https://www.twitonomy.com
(¹⁴) Here are some examples: https://miro.medium.com/max/360/1*mj0FpgxkM61lEftj4gzwAQ.png
     https://miro.medium.com/max/750/1*0e9Bwh-qgB0egnomovMg2w.png
(¹⁵) DFRLab has collected a set of clues that help to identify probable Kremlin accounts:
     https://medium.com/dfrlab/trolltracker-how-to-spot-russian-trolls-2f6d3d287eaa
     https://medium.com/dfrlab/russian-interference-the-evidence-fe6e52e50dcd

EU vs Disinfo

https://twitter.com/EUvsDisinfo

https://www.facebook.com/EUvsDisinfo/

https://euvsdisinfo.eu/

stratcom-east@eeas.europa.eu