EU vs Disinfo

ELECTION MEDDLING AND PRO-KREMLIN DISINFORMATION

WHAT YOU NEED TO KNOW

HOW DOES IT WORK?

METHODS OF FOREIGN ELECTORAL INTERFERENCE

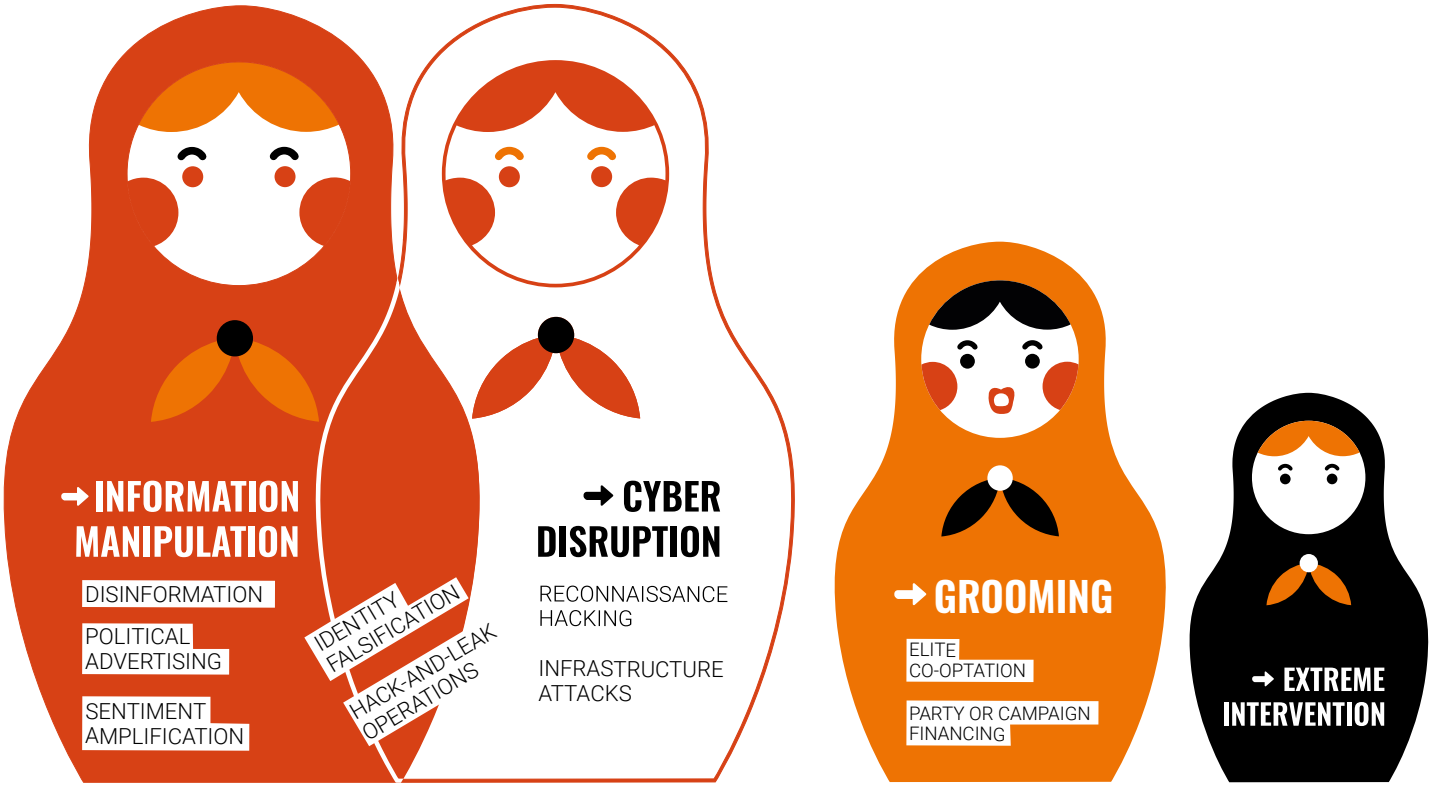
RUSSIA'S ELECTION MEDDLING TOOLKIT CONSISTS OF TEN KEY METHODS THAT FALL INTO FOUR CATEGORIES OF INTERFERENCE: A) INFORMATION MANIPULATION, B) CYBER DISRUPTION, C) POLITICAL GROOMING, AND D) EXTREME INTERVENTION.

➜ There is **no universal template** for the Kremlin's election meddling operations – every case is different and involves a **unique combination of methods** based on the Kremlin's objectives and the **specific context and vulnerabilities of the target country** or election process.

➜ Many of **these methods overlap and complement each other**, with the use of one indicating the likely use of another. For example, a phishing operation against a political campaign may suggest plans for a hack-and-leak operation. Social media influence campaigns typically involve both disinformation and sentiment amplification, sometimes combined with political advertising.

➜ **Russian electoral interference is a long game**: many of these methods are used, in varying degrees, far in advance of elections themselves, and only intensify during campaign periods. Influence efforts are now **a persistent feature of our political landscape**: for example, the Kremlin's disinformation war against Europe shows no signs of abating, while reports of cyberattacks are ever more common.

➜ **This long-term strategy of manipulation derives from the Soviet concept of "active measures"**: a slow process of ideological subversion and psychological warfare that aims, over many years, to alter the target's perception of reality and lead them to act in ways that benefit their opponent. The Kremlin's current and ongoing influence efforts are a sophisticated adaptation of this strategy for the digital era.



1. Disinformation

CLASS OF METHOD

→ Information manipulation

DEFINITION

The fabrication or deliberate distortion of news content aimed at deceiving an audience, polluting the information space to obscure fact-based reality, and manufacturing misleading narratives about key events or issues to manipulate public opinion. Disinformation is the most persistent and widespread form of the Kremlin's interference efforts. Importantly, it is not limited only to election cycles, but has now become a viral feature of our information ecosystem.

OBJECTIVE

To paralyse the democratic process by fuelling social fragmentation and polarisation, sowing confusion and uncertainty about fact-based reality, and undermining trust in the integrity of democratic politics and institutions.

CASE REFERENCES

- 2014 Ukrainian elections
- 2016 Dutch referendum on the EU-Ukraine Association Agreement
- 2016 Brexit referendum
- 2016 US elections
- 2017 Catalan independence referendum
- 2017 German elections
- 2017 French elections
- 2018 Italian elections

2. Political Advertising

CLASS OF METHOD

→ Information manipulation

DEFINITION

Using a fake identity or non-attributable false-front account to purchase online political ads, primarily on social media sites, to propagate disinformation about certain political parties, candidates, issues, or public figures.

OBJECTIVE

To promote and artificially inflate the (un)popularity of certain political parties, candidates, issues, or public figures in order to influence an election outcome.

CASE REFERENCES

- 2016 Brexit referendum
- 2016 US elections
- 2017 German elections

3. Sentiment Amplification

CLASS OF METHOD

- Information manipulation

DEFINITION

The use of fake accounts, trolls, and/or automated bots on social media and other online fora (e.g., the comments sections of newspapers) to spread disinformation and inflate the prominence of particular narratives. Sentiment amplification can occur both overtly (where the source is easily identifiable) and covertly (where the source is obscured or disguised to prevent correct attribution).

OBJECTIVE

To increase the proliferation and visibility of disinformation and related tendentious narratives in order to fuel social fragmentation and polarisation, sow confusion and uncertainty about fact-based reality, and undermine trust in the integrity of democratic politics and institutions.

CASE REFERENCES

- 2016 Brexit referendum
- 2016 US elections
- 2017 Catalan independence referendum
- 2017 German elections
- 2017 French elections
- 2018 Italian elections

4. Identity Falsification

CLASS OF METHOD

- Information manipulation
- Cyber disruption

DEFINITION

The establishment of a fake online identity, either by an individual or a group, which is used for false-front interaction with target audiences. Identity falsification can take numerous forms, including the creation of fake social media accounts to spread disinformation or run political ads, or the impersonation of specific individuals to conduct a sophisticated spear-phishing operation.

OBJECTIVE

Different forms of identity faking have different objectives. For instance, the purpose of creating a fake social media account may be to spread disinformation, organise an event, or incite a public reaction under the guise of an alternate identity in order to prevent attribution and create the illusion of authentic behaviour. The motive behind spear-phishing is the theft of user credentials in order to conduct a cyberattack.

CASE REFERENCES

- 2016 Brexit referendum
- 2016 US elections
- 2017 French elections (also here)
- 2017 German elections
- 2018 Italian elections

5. Hack-and-leak Operations

CLASS OF METHOD

- Information manipulation
- Cyber disruption

DEFINITION

The theft of emails or documents through hacking or phishing operations, followed by their strategic public release, typically via proxy to prevent attribution. The stolen documents may be altered (or additional ones fabricated) to manufacture greater controversy and increase negative perceptions of the target.

OBJECTIVE

To expose, disgrace, or otherwise undermine a particular individual, campaign, or organisation in order to influence public opinion during an election cycle.

CASE REFERENCES

- 2014 Ukrainian elections
- 2016 US elections
- 2017 French elections
- Germany 2018

6. Reconnaissance Hacking

CLASS OF METHOD
→ Cyber disruption

DEFINITION
Hacking operations against state institutions or publicly influential organisations such as think tanks, NGOs, and media organisations.

OBJECTIVE
To collect intelligence about these institutions' activities and research, to identify vulnerabilities for future exploitation, and to lay the groundwork for potential hack-and-leak operations.

CASE REFERENCES
- 2016 US elections (pre and post)
- 2018 Italian elections
- 2018 US elections
- 2019 European Parliament elections

7. Infrastructure Attacks

CLASS OF METHOD
→ Cyber disruption

DEFINITION
Infrastructure attacks encompass a variety of specific cyber tactics. Broadly, they involve any attempt to penetrate a country's electronic voting system, voter databases, or related IT networks. Specifically, these tactics may include distributed denial-of-service (DDOS) attacks, hacking of voter databases (either to gather information or to modify data), and manipulation of electronic vote transmission or vote counts in order to alter the election results.

OBJECTIVE
Motives vary in attacks on electoral infrastructure. They may include efforts to collect data for reconnaissance purposes or to identify vulnerabilities for future exploitation, to distort data (e.g., alter voter databases, manipulate votes), or to undermine the functionality of key IT systems or networks in order to weaken a particular party or candidate, or to broadly undermine the legitimacy of election results.

CASE REFERENCES
- 2014 Ukrainian elections
- 2015 German Bundestag attack
- 2016 US elections
- 2017 German elections

8. Elite Co-optation

CLASS OF METHOD
→ Grooming

DEFINITION
The cultivation of favourable relationships with key public- and private-sector elites. This relationship-building may take a number of forms, including business or trade incentives, academic and institutional influence via pro-Kremlin expert networks, "cooperation agreements" between political parties (the ruling United Russia party has several such agreements with European parties), and the use of individual operatives to infiltrate target circles (e.g., the case of Maria Butina in the US).

OBJECTIVE
To influence national decision-making and public opinion in the target country.

9. Party or Campaign Financing

CLASS OF METHOD
→ Grooming

DEFINITION
The overt or covert provision of funding to a particular party or election campaign, typically through a proxy institution without direct links to the Kremlin.

OBJECTIVE
To support and increase the chances of electoral success for a given party or candidate whose platform judged to benefit the Kremlin's agenda.

10. Extreme Intervention

CLASS OF METHOD

→ Extreme intervention

DEFINITION

The use of hard power to intervene in a country's political developments and democratic process, typically via overt or covert military action cushioned within a broader hybrid framework that violates the target country's territorial sovereignty.

OBJECTIVE

To directly alter the course of political developments in a target country, typically when other influence efforts have failed to yield the desired results.

CASE REFERENCES

- Georgia (2008, ongoing)
- Ukraine (2014, ongoing: annexation of Crimea, invasion of eastern Ukraine)
- Montenegro (2016 coup plot)

Direct vs. Indirect State Involvement

When evaluating and responding to a case of foreign election meddling, there are three levels of state involvement to consider: was the interference state-directed, state-sanctioned, or state-aligned?

STATE-DIRECTED INTERFERENCE

Interference activities that have either been financed or directly carried out by the government or other state institutions (such as the military or intelligence services).

STATE-SANCTIONED INTERFERENCE

Interference activities that are informally sanctioned or encouraged by the government or state organs, but not financed or directly carried out by the state.

STATE-ALIGNED INTERFERENCE

Interference activities that are carried out by non-state actors, without any apparent coordination with a foreign government, in support of that foreign government's agenda (e.g., independent hackers/hacktivists, homegrown disinformation sites that regurgitate pro-Kremlin narratives, etc.)

Distinguishing between these levels of state involvement in a given election meddling operation is vital for developing an effective response strategy. **State-directed and state-sanctioned interference efforts** require the most decisive action to punish the guilty state and deter future interference efforts.

Sources and Further Reading

- "Russian Election Meddling in the US and Beyond". (2018). EUvsDisinfo.
- "Election Interference in the Digital Age: Building Resilience to Cyber-Enabled Threats". (2018). European Political Strategy Centre of the European Commission.
- Galante, L. and Ee, S. (2018). "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents". Scowcroft Center for Strategy and Security, Atlantic Council.
- Laurinavičius, M. (2018). "A Guide to the Russian Tool Box of Election Meddling". International Elections Study Center.
- Brattberg, E. and Maurer, T. (2018). "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks". Carnegie Endowment for International Peace.
- Parks, M. (2018). "5 Ways Election Interference Could (and Probably Will) Worsen in 2018 and Beyond". National Public Radio.
- Greenberg, A. (2017). "Everything We Know About Russia's Election-Hacking Playbook". Wired.

HOW DOES IT WORK?

5 COMMON PRO-KREMLIN DISINFORMATION NARRATIVES

THE CONCEPT OF "NARRATIVES" COMES UP A LOT IN THE CONTEXT OF RUSSIAN AND PRO-KREMLIN DISINFORMATION AND INFLUENCE EFFORTS.

➜ A narrative is an overall message, communicated through texts, images, metaphors, etc. Repeatedly portraying individual politicians as crooks will eventually establish a narrativethat politicians generally are corrupt and deceitful.

➜ Pro-Kremlin disinformation outlets are using a set of narratives that works as templates for stories and can be adopted to a target audience. Different narratives are used for various audiences.

➜ Some of the narratives, used by disinformation outlets have been in use for hundreds of years. Variations of the narrative of "The Decaying West" can be documented since the 19th century.

➜ Narratives can be combined and modified based on current events and prevailing attitudes. Here is an overview of the five most common narratives that consistently appear in Russian and pro-Kremlin disinformation outlets.

HAHAGANDA

Used when confronted with compelling evidence or arguments – the reaction is to joke and mock it. The Kremlin has meddled in French elections in 2017? Haha, maybe the Kremlin is responsible for global warming and migration crisis, too?

THE ELITES VS. THE PEOPLES

Used to show conspiracies around you: bankers/big corporations/-Jews/oligarchs/Muslims/Brussels bureaucrats. They are all conspiring against us, the people. But there is only one person or one party that knows the truth, and you should trust only them.

SOVEREIGNTY LOST

Used to suggest that someone other than you think is ruling your country: Ukraine is ruled by foreigners, Baltic States are not really countries, the EU is directed by Washington

THREATENED VALUES

Used to condemn Western values: for example, those advancing rights of women, ethnic and religious minorities and LGBTQ groups, are a threat to "tradition", "decency", and "common sense".

EVERYTHING WILL COLLAPSE

Used to suggest that the end of the Western world is coming and you are helpless: the EU is dissolving, NATO is breaking down, Western economy is collapsing.

1. The Elites vs. the People

THIS NARRATIVE, BROADLY BASED ON THE IDEA THAT "EVIL ELITES" ARE OUT OF TOUCH WITH THE NEEDS OF THE "PEOPLE", IS A COMMON POPULIST TROPE THAT CAN BE ESPECIALLY POWERFUL DURING ELECTION CYCLES.

We have seen it many times before: a party or a candidate, claiming to be the "voice of the people" or "the silent majority", deploys this narrative to attack the political establishment and offers voters easy solutions to complex problems. This narrative can be very successful as it provides a scapegoat for the target audience to blame for any grievances: bankers, Big Corporations, Jews, oligarchs, Muslims, Brussels bureaucrats. Russian and pro-Kremlin disinformation outlets heavily exploited this narrative on the eve of the 2016 Brexit referendum, as these two Sputnik articles demonstrate: "The Threat from Eurocracy threatens Europe" and "Waffen-EU". Both stories resonated strongly with the Leave campaign.

Questioning the legitimacy of the electoral process is also a common characteristic of this narrative. Sputnik, for example, frequently "reports" about alleged election fraud, underscoring the idea that elites manipulate elections. Here are examples about Germany (in German), Sweden (in Russian), and Ukraine (in Russian).

The Elites vs. People narrative has a long, over hundred-year history. Its purveyors claim to be a voice of reason and to advocate on behalf of disenfranchised citizens, speaking truth to power against elites that seek to hide the "truth" at any cost. The "truth" can relate to a broad variety of issues, including migration, politics, and the economy; while the particular elites deemed "guilty" of hiding the truth are strategically selected to suit the grievances of the target audience. Indeed, this narrative can be adapted and applied to a seemingly infinite number of issues: "The migration crisis is caused by big corporations in order to obtain cheap labour"; "The Global Warming Hoax is used by bankers to divert public attention from real-world problems". The list goes on and on...

Ultimately, while this narrative appears on its surface to sympathise with ordinary people, its roots are in fact strictly authoritarian. Evidence is rarely provided to substantiate the claims made and, following the principles of conspiracy thinking, the very absence of evidence is sometimes used as proof: "See how powerful the elites are, hiding all trace of their conspiracy!" Typically, this narrative also demands that the reader rely exclusively on the word of the narrator: "I know the truth, trust me!" Indeed, like all narratives based on conspiracy theories, this one requires its audiences to accept the claims on the basis of faith rather than fact.

2. Threatened Values

THE NARRATIVE ABOUT "THREATENED VALUES" IS ADAPTED TO A WIDE RANGE OF TOPICS AND TYPICALLY USED TO CHALLENGE PROGRESSIVE WESTERN ATTITUDES ABOUT THE RIGHTS OF WOMEN, ETHNIE AND RELIGIOUS MINORITIES, AND LGBTQ GROUPS, AMONG OTHERS.

According to this narrative, the "effeminate West" is rotting under the onslaught of decadence, femenism and "political correctness", while Russia embodies traditional paternal values. This narrative is depicted in a 2015 cartoon by Russian state news agency RIA Novosti, illustrating Europe's apparent moral decay: from Hitler, to sexual deviance, to a future of rabid hyenas. Value-based disinformation narratives usually centre on threatened concepts like "tradition", "decency", and "common sense" – terms that all have positive connotations but are rarely clearly defined. The narrative creates an "Us vs. Them" framework which suggests that those who are committed to traditional values are now threatened by those who oppose them and instead seek to establish a morally bankrupt dystopia. Russian and pro-Kremlin disinformation outlets pushed variations of this narrative in the run-up to the 2018 Swedish general election, as can be seen here and here. In Russian-language outlets, like the infamous St. Petersburg Troll Factory News Agency RIAFAN, the language of this narrative is particularly aggressive: "What it is like in the country of victorious tolerance: Gays and lesbians issue dictates, oppression of men and women, Russophobia and fear"

By contrast to the Western conception of values, which favours individual rights of personal integrity, safety, and freedom of expression, the Russian value system entails a set of collective norms that every individual is expected tp conform to. Yet the narrative is always expressed from a position of moral high ground, in which the silent majority, committed to decency and traditionalism, is under attack from liberal "tyranny". The target audience is invited to join the heroic ranks that are boldly fighting for family values, Christianity, and purity.

3. Lost Sovereignty, or Threatened National Identity

RUSSIAN AND PRO-KREMLIN DISINFORMATION SOURCES LIKE TO CLAIM THAT CERTAIN COUNTRIES ARE NO LONGER TRULY SOVEREIGN. RUSSIAN STATE NEWS AGENCY RIA NOVOSTI ILLUSTRATES THIS IDEA WITH A CARTOON: UNCLE SAM IS TURNING UP THE FLAME ON A GAS STOVE, FORCING EUROPEANS TO JUMP UP AND DOWN AND CRY FOR SANCTIONS (AGAINST RUSSIA, THAT IS).

Examples of this narrative are numerous: Ukraine is ruled by foreigners and the Baltic states are not really countries. The EU is directed by Washington. NATO and the EU are pursuing militaristic and bureaucratic ambitions, disregarding the interests of their member states and, of course, their citizens – sometimes not even by intent, but simply through incompetence or being out of touch with reality. You can decide which explanation is worse – ineptitude or malicious intent.

Closely related to this narrative of lost sovereignty is that of a threatened national identity, where existential danger stems from a diverse array of sources: Islam, gay people, children's rights, and more.

Recent events suggest that these narratives can have a strong impact on audiences. European governments only accept instructions from NATO, Brussels, and Washington. Europe is occupied by the US. Germany is no longer a sovereign state. European cooperation between national governments is depicted as state capitulation to foreign rulers.

This narrative has been successfully employed in several European elections and referenda. Convincing voters that their grievances are the result of resources being funnelled to "others" – foreigners, bankers, corporations, minorities – has proven to be an efficient manipulation strategy. Indeed, combined with fuelling nostalgia for a mythical national past, this narrative is one of the most damaging disinformation strategies out there. It has been deployed in connection with the Catalan independence referendum, Brexit, and in several national elections.

4. Everything Will Collapse

AS MENTIONED ABOVE, RUSSIA HAS BEEN FORESHADOWING EUROPE'S IMMINENT COLLAPSE FOR WELL OVER A CENTURY. DESCRIBING EUROPE OR EU MEMBER STATES AS "ON THE VERGE OF CIVIL WAR" WORKS JUST AS WELL IN 2019 AS IT DID IN 1919.

This is a hard-working narrative that usually resonates well with target audiences, despite the fact that Europe has not collapsed and, by many metrics, continues to flourish.

The narrative is employed regularly by Russian and pro-Kremlin disinformation outlets: The EU Superstate is collapsing, US economy is collapsing, NATO is breaking down, the Yellow Vest movement is destroying the banking system. The RIA Novosti cartoonist describes terrorism in Europe as a deadly scorpion that Europeans have unwittingly placed in their pocket.

Target audiences that – legitimately or not – already fear political and social turmoil in their countries are particularly susceptible to this narrative.

Thus, this narrative works especially well during periods of real political challenge, like during the migration crisis in the fall of 2015. The enormous influx of migrants to Europe certainly posed a major challenge to European governments, but the Russian and pro-Kremlin media portrayed the situation in grossly overstated and apocalyptic terms, reporting about the crisis as though it constituted a systemic collapse. Of course, the system survived intact, but the image of Collapse lingers on.

The same approach is visible in Russian and pro-Kremlin coverage of the Yellow Vest protests in France. The right to express discontent with government and politics is an integral part of democracy, and the citizens of any European state enjoy the right to take to the streets. The Yellow Vest movement belongs to the European democratic tradition, and is not proof of the breakdown of the system.

This narrative is also sometimes used to lament the alleged breakdown of European moral values and traditions. Russian and pro-Kremlin disinformation outlets for instance regularly describe children's rights in Europe as an attack on family values. Europe is dying, abandoning all decency and morals.

5. The *Hahaganda* Narrative

A FINAL RESORT IN DISINFORMATION, TYPICALLY WHEN CONFRONTED WITH COMPELLING EVIDENCE OR ARGUMENTS, IS TO JOKE ABOUT THE SUBJECT. THE SKRIPAL CASE IS AN EXCELLENT EXAMPLE OF THIS STRATEGY. RUSSIAN AND PRO-KREMLIN DISINFORMATION OUTLETS HAVE ATTEMPTED TO DROWN OUT THE ASSASSINATION ATTEMPT WITH SARCASM TO TURN THE ENTIRE TRAGEDY INTO ONE BIG JOKE.

More generally, in connection with elections, this method involves the use of various derogatory words to belittle the concept of democracy, democratic procedures, and 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. Ukrainian President Petro Poroshenko is almost constantly ridiculed in pro-Kremlin media, as is Ukraine's entire election process. According to Russian state media, an election with several candidates and no obvious outcome is considered a circus.

Of course, satire, humour, and parody are all integral components of public discourse. The right to poke fun at politicians or make jokes about bureaucrats is important to the vitality of any democracy. It is ironic, then, that Russian and pro-Kremlin disinformation outlets often seek to disguise their anti-Western lies and deception behind a veil of satire, claiming it is within their rights of free speech, while aggressively refusing to tolerate any satire that is critical of the Kremlin or undermines its political agenda. An example of this hypocrisy is Russia's ban on the 2018 British comedy The Death of Stalin.

In a 2017 report, NATO's StratCom Centre of Excellence published a report explaining how Russian and pro-Kremlin disinformation outlets use humour to discredit Western political leaders. One of its authors, the Latvian scholar Solvita Denise-Liepnice, has suggested the term "*hahaganda*" for this particular brand of disinformation, which is based on ridiculing institutions and politicians. The goal of hahaganda is not to convince audiences of the truth of a particular joke, but rather to undermine the credibility and trustworthiness of a given target via constant ridicule and humiliation.

Summary: United in Disempowerment

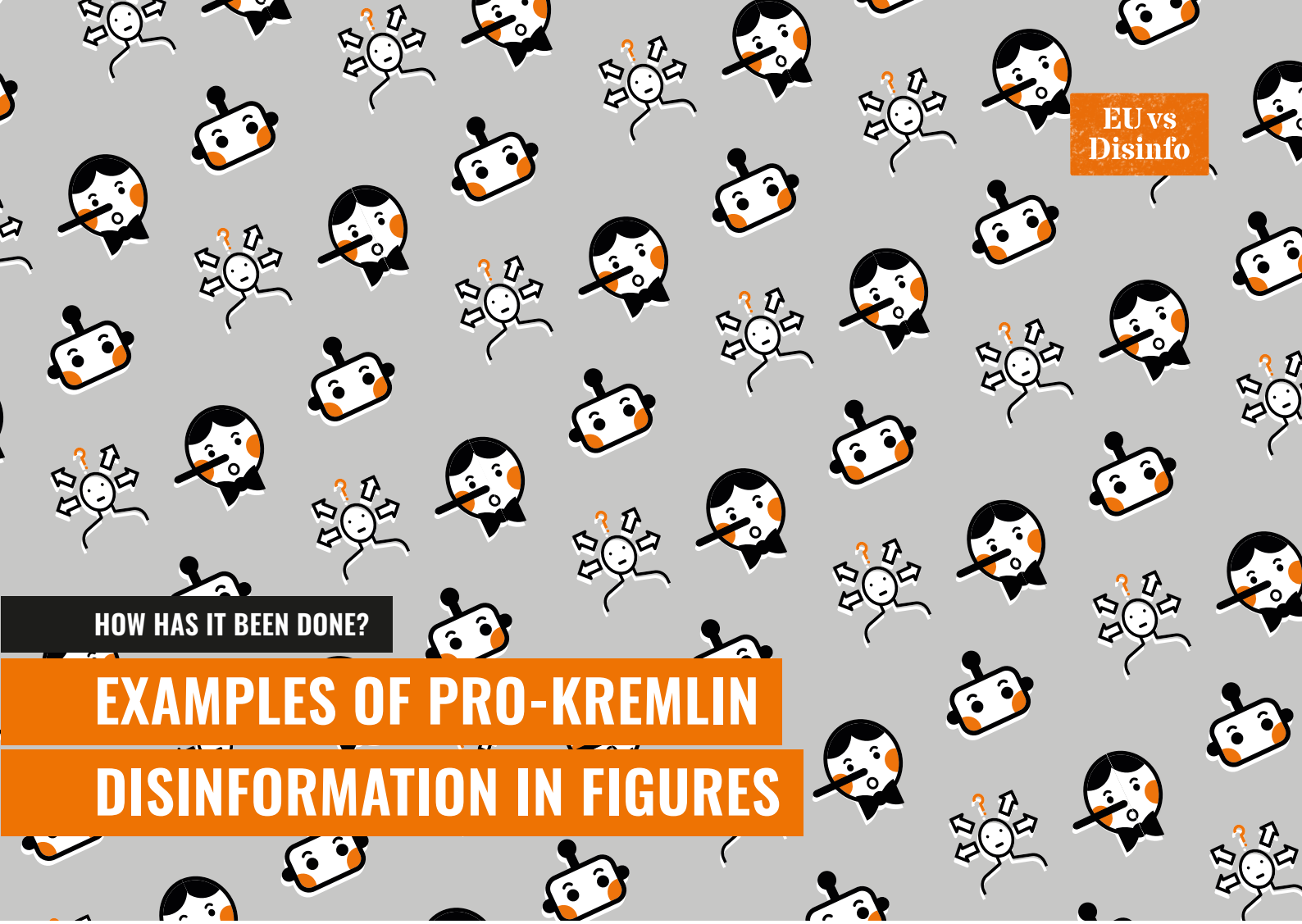
THE FIVE NARRATIVES, AS WE CAN SEE, ARE CLOSELY RELATED AND SHARE THE OVER-ARCHING THEME OF DISEMPOWERMENT DRIVEN BY "EVIL ELITES". NATIONAL GOVERNMENTS ARE WEAK AND INEFFECTUAL; CITIZENS ARE DISENFRANCHISED, THEIR TRADITIONS FACE DESTRUCTION – AND BY WHOSE HAND?

Bureaucrats in Brussels, corporate businessmen, shadow rulers, and of course, fascists! In contrast to this chaos, insecurity, and moral decay across Europe and the West, Russia is depicted as a source of paternal security and stability. In fact, leading Russian voices even advocate Russia's regime of "enlightened authoritarianism" as an ideal political system for the future.

Another shared feature of these major narratives is that they attack Western democratic institutions and legal systems in order to foster distrust and social fragmentation, with the ultimate goal of subverting democracy. This strategy of cultivating distrust is designed to convince citizens that their participation in the democratic process is meaningless: voting is futile because the system is "rigged" in favour of elites and only exploits ordinary citizens. Thus, democracy is portrayed as a farce that is moreover inefficient and ill-suited to address contemporary challenges.

Ultimately, most pro-Kremlin disinformation narratives simply recycle the same tropes over and over again in different combinations. Give it a try with the do-it-yourself narrative matrix:

WHO IS	DOING WHAT	WITH WHAT	TO WHOM	FOR WHAT PURPOSE
The Establishment is	importing	migrants to	Europe	as cheap labour
George Soros is	financing	the opposition in	Hungary	to orchestrate a coup
The Jews are	scheming with	the Deep State in	the whole world	to gain supremacy
The mainstream media are	lying about	climate change in	Venezuela	to please their masters
The feminists are	in cahoots with	the Muslims in	Germany	to castrate real men
The military-industrial complex is	creating Russophobia through	the mainstream media in	the Baltics	to maximise profit
The Rothschilds are	supporting	the Yellow Vests in	France	to oppress the working people
Trump is	battling	the big corporations in	the USA	to get even richer
The Vatican is	conspiring with	feminists from	Sweden	to destroy the traditional family
The Pentagon is	secretly testing	chemical weapons in	Georgia	to kill orthodox Christians
Fascists are	disguising themselves as	liberals in	the West	to break up Russia



HOW HAS IT BEEN DONE?

EXAMPLES OF PRO-KREMLIN DISINFORMATION IN FIGURES

The Kremlin's electoral meddling has many different forms around the world. In several recent European elections, we have seen a variety of interference tactics, including personal attacks, hack-and-leak operations, false narratives, playing on sentiments, cyberattacks, and more.

Of these methods, information manipulation remains a particularly pervasive tactic. Malign actors prefer techniques of information manipulation, as they are effective and not expensive.

As the Kremlin's tactics evolve, research into their scope and impact is growing. We have collected some figures and data from recent European elections and referenda that illustrate the scope of this threat.

Common Information Manipulation Tactics

➜ Pro-Kremlin actors use a variety of information manipulation tactics to influence elections. On the one hand, they **propagate certain disinformation narratives** – in the case of Catalonia, for example, that Spain and Europe are in deep crisis – and **try to amplify negative sentiments** that are already present in discussions.

➜ In other cases, for example German parliamentary elections in 2017, the meddlers **side with a particular candidate or political party,** and they seek to boost public support for their sake. Meanwhile, ahead of Italy's 2018 parliamentary elections, pro-Kremlin actors tried to amplify anti-migration messages, and successfully spread them primarily through anti-immigration communities.

➜ Finally, another common tactic is to **create chaos and confusion** by promoting contradictory narratives from both sides of a political issue, as exemplified in the 2016 Brexit referendum. Even though the Kremlin explicitly promoted the Leave campaign, Russia-linked Twitter accounts in fact spread both pro- and anti-Brexit narratives in the run-up to the referendum.

Amplification via Bots

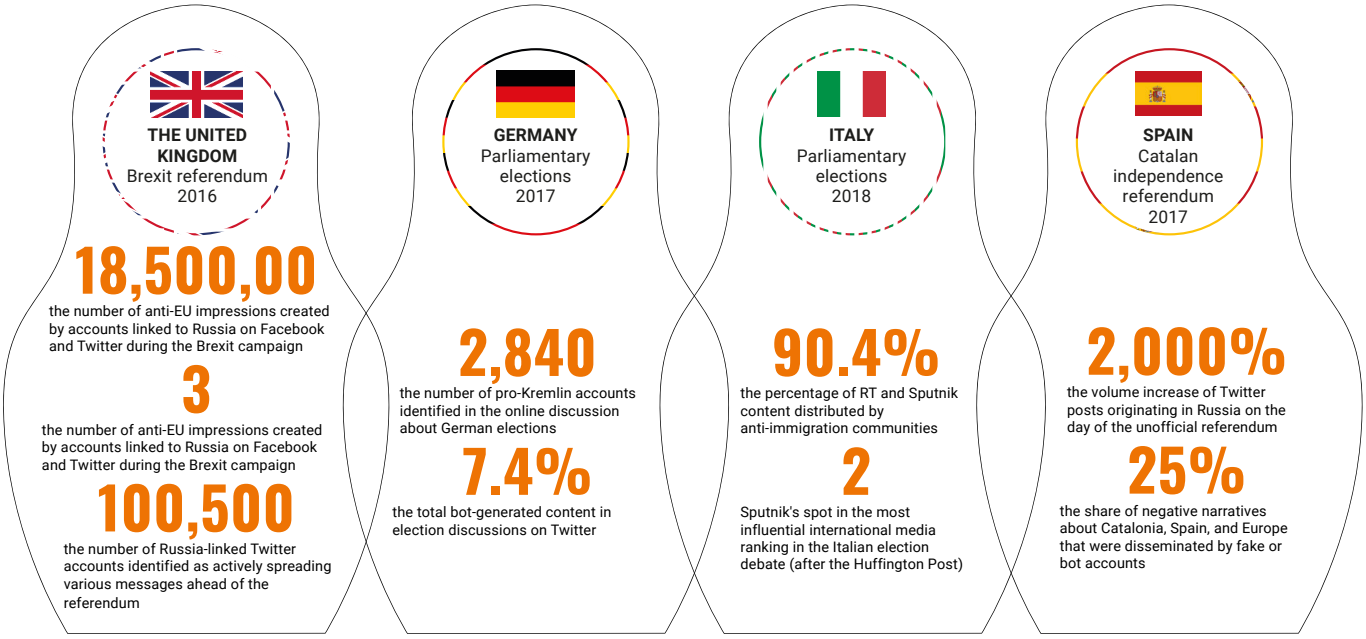
➜ Research shows that automated bots on social media play a significant role in election meddling. For instance, bots contributed to the rampant spread of anti-EU messages on British social media.

➜ Bots constituted one fourth of the accounts that spread the leading pro-Kremlin narratives during the unofficial Catalan referendum.

Manipulating Traditional Media

➜ Complementing the social media tactics, pro-Kremlin actors rely on the manipulation of traditional media, namely by **planting disinformation and deceptive narratives** with help of pro-Kremlin outlets. Those narratives are then picked up by other sources and can gradually gain mainstream legitimacy.

➜ This approach was effective in several cases: articles by RT and Sputnik were among the most shared in Spain around the unofficial Catalan referendum. Similarly, RT and Sputnik ranked in the top 3% of the most influential media outlets in Italy ahead of the 2018 national elections.



Sources and Further Reading:

- *The Brexit Botnet and User-Generated Hyperpartisan News,* University of London, Social Science Computer Review, October 2017 https://journals.sagepub.com/doi/10.1177/0894439317734157
- *Putin's Assymetric Assault on Democracy in Russia and Europe: Implications for US National Security, A Minority Staff Report prepared for the Committee on Foreign Relations United States Senate,* January 2018 https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf
- *Putin's Brexit? The influence of Kremlin media & bots during the 2016 UK EU referendum*, 89up, February 2018 http://89up.org/russia-report
- *Disinformation and 'fake news': Interim Report,* UK Parliament Select Committee, July 2018 https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm
- Analyses by DFR Lab on disinformation around federal elections in Germany in 2017:

https://medium.com/dfrlab/far-right-targets-germany-on-reddit-ba8b2f379b8b https://medium.com/dfrlab/electionwatch-german-fringe-media-targets-russian-social-media-platform-7cd5549e0179 https://medium.com/dfrlab/electionwatch-final-hours-fake-news-hype-in-germany-cc9b8157cfb8

- *'Make Germany Great Again'. Kremlin, Alt-Right and International Influences in the 2017 German Elections*, Institute for Strategic Dialogue, Institute of Global Affairs, London 2017 https://www.isdglobal.org/wp-content/uploads/2017/12/Make-Germany-Great-Again-ENG-061217.pdf
- *Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?,* The Computational Propaganda Project, September 2017 https://comprop.oii.ox.ac.uk/research/junk-news-and-bots-during-the-german-parliamentary-election-what-are-german-voters-sharing-over-twitter/
- *The construction of anti-immigration electoral messages in Italy, Alto Data Analytics,* https://www.alto-analytics.com/en_US/the-construction-of-anti-immigration-messages-in-italy/
- *Russian TV's view on Catalonia referendum: Europe falling apart and Spain compared to Ukraine*, EUvsDisinfo, October 2017 https://euvsdisinfo.eu/russian-tvs-view-on-catalonia-referendum-europe-falling-apart-and-spain-compared-to-ukraine/
- *Russian network used Venezuelan accounts to deepen Catalan crisis*, El Pais, November 2017 https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html
- *The 'combination': an instrument in Russia's information war in Catalonia, Real Instituto Elcano,* November 2017 http://www.realinstitutoelcano.org/wps/wcm/connect/147fabf2-1140-499d-a59f-150c1eba8026/ARI92-2017-MilosevichJuaristi-Combination-instrument-Russia-information-war-Catalonia.pdf?MOD=AJPERES&CACHEID=-147fabf2-1140-499d-a59f-150c1eba8026
- *US Senate report condemns Russian interference in Catalan referendum*, El Pais, January 2018 https://elpais.com/elpais/2018/01/11/inenglish/1515667883_820857.html

HOW HAS IT BEEN DONE?

TACKLING DISINFORMATION À LA FRANÇAISE

MEDDLING IN THE 2017 FRENCH ELECTIONS IS A SHOWCASE OF DIFFERENT METHODS IN THE KREMLIN PLAYBOOK: A MIXTURE OF PERSONAL ATTACKS, FALSE NARRATIVES, AS WELL AS HACKS AND LEAKS (OF REAL AND FAKE DOCUMENTS). BUT IT IS ALSO A STORY ABOUT HOW A QUICK AND TRANSPARENT REACTION, COMBINED WITH BROAD COOPERATION, CAN HELP CONTROL THE DAMAGE.

What, How, and Why?

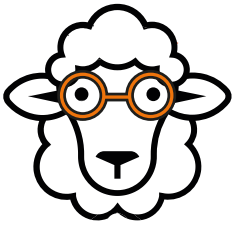
VARIOUS ANALYTICAL INSTITUTIONS MADE IT CLEAR: THE KREMLIN PLAYED A KEY ROLE IN MEDDLING IN FRANCE'S 2017 PRESIDENTIAL ELECTIONS. AT THE SAME TIME, SOME RESEARCHERS SUGGEST THAT THE KREMLIN MIGHT NOT HAVE BEEN THE ONLY ACTOR RESPONSIBLE.

The purpose of meddling was to advance one of the candidates which the Kremlin counted on to have a more positive stance towards Russia. Nevertheless, Russia denied any involvement.

Meddling in the 2017 French elections is now mostly associated with the so-called 'Macron Leaks'. In this case, 9 GB of data were hacked from computers of Emmanuel Macron's campaign staff, including the candidate himself. This might have been the most prominent example of interference – but it certainly wasn't the only one.

In the first months of 2017, when the presidential election campaign was starting to gather pace, pro-Kremlin outlets were much keener on reporting positively about Francois Fillon and Marine Le Pen, as a DFR Lab study shows.

INVOLVED PRIVATE ACTORS (FOR EXAMPLE DIGITAL PLATFORMS)



INFORMED, CRITICALLY THINKING CITIZENS

INDEPENDENT, CREDIBLE, AND DATA-ORIENTED JOURNALISTS

LESSONS LEARNED FROM FRANCE

WHAT DO WE NEED TO TACKLE DISINFORMATION IN ELECTIONS?

STRONG INSTITUTIONS

COOPERATION BETWEEN ALL INVOLVED

At the same time, the biggest wave of criticism, incomparable with what other candidates were faced with, was directed at Emmanuel Macron. Opinions about the candidate's lack of vision or programme are a rather usual thing – but in this case, RT and Sputnik stopped at nothing short of mockery and personal attacks. Narratives varied from describing Macron as a pure marketing product, to his alleged "homosexual orientation", to being an American spy, to being supported by Saudi Arabia and the Rothschilds. And this line of disinformation attacks became stronger as Macron started advancing in the polls.

This kind of smearing and disinformation campaign is a classic in the Kremlin's playbook. It is also standard to diversify the attacks, narratives, and areas of action to make the meddling efforts more effective. This is why the campaign against Macron did not stop at the level of media and social media. It also went deeper underground and into cyberspace. First, already at the outset of 2017, email accounts of Macron's close collaborators were hacked. But it took long enough to make the hacked data public. The data leaks occurred in the last hours of the second round of the presidential campaign – right before the purdah period, when media and candidates have to refrain from electoral agitation. The #MacronLeaks managed to go viral just before that, with a mixture of real emails exchanged between campaign employees and absurd fake messages. A few days before that, a different series of false messages was activated under the #MacronGate hashtag – this time, they were based on two fake documents and which were supposed to prove that Macron has a secret offshore account.

In a nutshell, the strategy was as follows: to spread many false narratives with the help of different methods and tools – and then wait for them to be amplified, first with help of 'hacktivists' and the 'cyber underground', then social media and finally the traditional media. There was also the expectation that, in the meantime, ordinary citizens would get involved too. The whole strategy was not solely about discrediting one of the candidates; it was also about sowing doubt about democracy, the leadership, and one's ability to exert any influence on the democratic system.

The Response

PERSONAL ATTACKS, HACKING, FALSIFYING DOCUMENTS, DISINFORMATION, FALSE NARRATIVES – IN THE 2017 FRENCH ELECTIONS, EVERYTHING WAS THERE. NEVERTHELESS, IF THE AIM OF MEDDLING WAS FOR EMMANUEL MACRON TO LOSE THE ELECTION, APPARENTLY IT DID NOT SUCCEED. WHAT WENT WRONG FOR THE KREMLIN?

The strategy applied in France could be summarized in three words: reaction, preparation, cooperation.

First of all, meddling attempts met with reactions from across different sectors.

The then presidential candidate Emmanuel Macron and his campaign aides were clear in labeling RT and Sputnik as pro-Kremlin disinformation outlets. After Macron was elected, they have not become part of the press corps at the Élysée Palace and have been regularly refused to cover official events.

Also, legal steps were taken: In December 2018, a new law was adopted with the aim to fight the spread of disinformation.

French journalists did not let disinformation fool them – they did their job and checked the sources, claims and messengers conveying them. Thus, they responded with research and reliable data. For example, the 'Macrongate' story was quickly debunked by The Observers (a collaborative project under the umbrella of France 24). Other journalists followed suit. The story did spread across social media, but without the quick reaction of the media, it could have become a mainstream narrative.

In the case of the Macron Leaks, the environment of the presidential candidate reacted quickly, too. On the one hand, they did confirm that real emails and messages were indeed part of the leak. On the other, they used the lively environment of social media to engage in conversations about it, with a clear narrative about the content of the leak: they were, actually, part of the usual actions taken during an election campaign.

Emmanuel Macron's campaign staff also used the opportunity to do something out of the box: play with those who were behind the hacks and leaks. They planted some absurd false messages and documents in their own networks, in order to confuse the hackers and burden them with the necessity to explain why they leaked false information.

How was it possible to do the latter? Because the campaign staff actually anticipated that their computers and communications will be hacked. And that, in turn, was possible thanks to their cooperation with digital platforms and state institutions. The latter is of crucial importance here, as strong institutions are fundamental to secure the democratic process in France.

Moreover, France learned from the experience of other countries, especially the 2016 American elections. It could therefore prepare different scenarios and reactions as well as adapt the experience of others to its own situation.

The essential element of raising public awareness was included in the reaction, too. Here, again, French institutions played their part. For example, they continuously informed citizens about the risk of disinformation and cyberattacks and offered workshops for campaign staff. Everybody thus had the opportunity to prepare.

All in all, knowledge that meddling will happen made it possible for the institutions and campaign staff to prepare for different scenarios and make everybody aware of the risks. This, in turn, became real because none of the actors involved in the election process operated in a vacuum – information was exchanged and resources activated across governmental and non-governmental networks. Finally, a quick and transparent reaction ensured that the truth was out there, providing citizens with all resources needed to make an informed choice.

Further Reading

- "In France, RT Is Getting No Love". (2018). EUvsDisinfo.
- "Information Manipulation. A Challenge to our Democracies". (2018).The Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) and The Institute for Strategic Research (IRSEM, Ministry of the Armed Forces).
- Popescu, N. and Secrieru, S. (2018). "Hacks, Leaks and Disruptions: Russian Cyber Strategies". Chaillot Papers No. 148, EU Institute for Security Studies.
- Conley, H. and Vilmer, J. J. (2018). "Successfully Countering Russian Electoral Interference". Centre for Strategic and International Studies.
- Aaltola, M. (2017). "Democracy's Eleventh Hour: Safeguarding Democratic Elections against Cyber-Enabled Autocratic Meddling". Finnish Institute of International Affairs.
- "The French Election Through Kremlin Eyes". (2017). DFR Lab, Atlantic Council.
- "How We Debunked Rumours that Macron has an Offshore Account". (2017). The Observers, France 24.

HOW HAS IT BEEN DONE?

HOW THE ST. PETERSBURG TROLL FACTORY TARGETS ELECTIONS FROM GERMANY TO THE UNITED STATES

THE ST. PETERSBURG "TROLL FACTORY", ALSO KNOWN AS INTERNET RESEARCH AGENCY (IRA), HAS BECOME A CENTRAL PART OF THE KREMLIN'S ELECTORAL INTERFERENCE PLAYBOOK.

➜ The IRA has been actively exporting the Kremlin's disinformation tactics abroad since 2013, targeting numerous elections and referenda in Europe and the US.

➜ Altogether, the funding for the US operation between January 2016 and June 2018 was approximately 35 million USD.

➜ The IRA remains active in its online manipulation efforts, with experts warning that Russian trolls are adapting their strategies to circumvent new protections implemented by social media companies.

SINCE ITS INCEPTION, THE ST. PETERSBURG TROLL FACTORY HAS HAD A SPECIFIC FOCUS ON ELECTION INFLUENCE OPERATIONS.

In 2014, local elections were scheduled to take place in St. Petersburg, Russia. However, well in advance of election day, some of the city's residents began receiving unexpected visitors knocking at their doors. The guests presented themselves as journalists from the newspaper *Nevskie Novosti* and said they were conducting interviews: "Which politicians do you support? What are the biggest problems in your neighbourhood?"

In fact, the "journalists" were anything but – they were analysts from one of several projects established by the Internet Research Agency (IRA): the now-infamous St. Petersburg troll factory, and the newspaper was and is run by it. The objective of the analysts' canvassing and interview efforts was to collect information that could be used to ensure a win for the ruling party, United Russia, and to assess

which candidates would likely need vote count "corrections" by way of election fraud.

While this operation was ongoing, the troll factory was already openly hiring English-speaking specialists.

Heading into the 2019 European elections, our understanding of the troll factory's operational scope, objectives, and methods is significantly greater than it was just a few years ago. We know that the physical operation has now grown to three times its starting size, occupying 12,000 square meters in the Lakhta business district, although recent reports indicate that one of its company affiliates has allegedly left the office space. The troll factory has successfully created a whole network of popular Russian-language media outlets boasting dozens of millions of readers every month.

The organisation is controlled by the Russian businessman Yevgeny Prigozhin, who runs a number of other ventures on the side, including catering services for Russian schools and the army, as well as private military companies that are currently operating in Ukraine and Syria. Unsurprisingly, given this resumé, Prigozhin has also been linked to violent attacks against bloggers and opposition activists who are critical of the Kremlin.

As several recent election cycles in Europe and the US have shown, the troll factory is highly adept at exporting the Kremlin's disinformation tactics abroad, conducting complex online influence operations to sway elections and manipulate public opinion. And it shows no signs of slowing down – on the contrary, faced with new protections by social media companies to prevent the spread of disinformation on their platforms, the trolls are beginning to adapt their influence strategies to find ever newer ways of spreading their venom.

Six Years of Exporting Disinformation to the US

On june 27, 1952, American government passed a law, called "1952 McCarran Walters act", that actually outlawed Sharia, but Obama never intended to enforce it or even let you know about it at all. Instead he started to import thousands of aggressive Muslim "refugees", who refused to integrate and demanded to be allowed to live under sharia law instead of American constitution. Now it's within Donald Trump's authority to enforce that law and ban Sharia in every state across America. Do you want him to do that?

Image source: IRA Facebook post, posted by the Stop A.I. page in January 2017 (total shares: 312,667)

ATTEMPTS TO MANIPULATE US VOTERS BEGAN IN 2013 BUT ESCALATED RAPIDLY IN 2014, STARTING ON TWITTER AND SUBSEQUENTLY SPREADING TO YOUTUBE, INSTAGRAM, AND FACEBOOK.

Just few weeks before the 2016 presidential election, the department dedicated to the US operation already had more than 80 employees and a monthly budget of 1.25 million USD. Between 2013 and 2018, the IRA's Facebook, Instagram, and Twitter campaigns reached tens of millions of users across the United States.

In the run-up to the 2016 election, the troll factory's activities were aimed at polarising the US electorate by exploiting existing fault lines and hot-button partisan issues, including race relations, LGBT rights, gun rights, immigration, and more. The trolls produced content encouraging **African American voters to boycott elections** and follow **wrong voting procedures**, incited **extreme right-wing voters** to be more confrontational, and spread disinformation on a wide range of issues to voters on both ends of the political spectrum.

In tandem with the troll factory operation, Russia's military intelligence service, the GRU, hacked several key Democratic groups and stole caches of emails and documents. Then, creating false online personas and websites – and in cooperation with Wikileaks – the GRU strategically released tens of thousands of these documents at key moments during the campaign in an apparent attempt to maximise damage to Hillary Clinton and, in turn, boost support for Donald Trump.

The troll factory also understood the power of local news: the IRA created a number of Twitter accounts that posted **real local news,** serving as sleeper accounts aimed at building trust and readership that could be exploited in future influence operations. Twitter suspended the accounts before they were used for disinformation purposes.

After the 2016 US election, the troll factory's engagement efforts increased in both scope and intensity, expanding to target new audiences and to cover a broader range of issues. Younger voters were targeted, along with Mexican American and Hispanic voters, with efforts to increase their distrust in US institutions.

The peak of the troll factory's advertising volume on Facebook was in April 2017: a period that coincides with the Syrian missile strike, the use of the "Mother of All Bombs" on ISIS tunnels in Afghanistan, and the release of the US tax reform plan.

In 2018, the US operation intensified once again, when the budget was increased to 10 million USD for January to June. Altogether, the funding for the US operation totalled 35 million USD from January 2016 to June 2018.

At least 50,000 homeless veterans are starving dying in the streets, but liberals want to invite 620,000 refugees and settle them among us. We have to take care of our own citizens, and it must be the primary goal for our politicians!

Image source: IRA Facebook post, posted by the page Being Patriotic on September 8, 2016 (total shares: 640,390)

Focus on Europe: Netherlands, Brexit, and Germany

THE TROLL FACTORY'S ACTIVITIES HAVE NOT BEEN LIMITED TO THE US, BUT HAVE TARGETED NUMEROUS EUROPEAN ELECTIONS FROM THE NETHERLANDS TO GERMANY. IRA ACCOUNTS ALSO PROMOTED THE DATA DUMP FROM THE HACK-AND-LEAK OPERATION AGAINST FRENCH PRESIDENT EMMANUEL MACRON DURING HIS ELECTION CAMPAIGN.

Image: Tweet by an IRA account after the London terror attack in March 2017, which was cited by The Sun and Mail Online. The IRA continued stirring up anti-Islamic sentiment after Brexit.

Before the Dutch went to the polls for a referendum on the EU-Ukraine association agreement in 2016, the troll factory spread **a fake video about Ukrainian far-right ultra-nationalist** Azov battalion fighters, who allegedly threatened to carry out terrorist attacks in the Netherlands should the referendum be rejected and were burning the Dutch flag.

In the UK, the strategy focused **on stoking anti-Islamic sentiment ahead of the Brexit vote**. The most-retweeted tweet in the six months running up to the referendum was "London: Muslims running a campaign stall for Sharia law! Must be sponsored by @MayorofLondon!"

Prior to Brexit, the troll factory began building its audience base by tweeting about innocuous topics like health and fitness to remain under the radar (similar to what it attempted with local news in the US), and later switched its focus to political messaging. On the day of the referendum, its tweets were generally anti-EU, but also included messages such as: "Algerian illegally in Britain attacked 8 women in ten days! Send the Muslim back to EU!" and, from a fake US account, "I hope UK after #BrexitVote will start to clean their land from muslim invasion!".

On a wide range of topics, IRA accounts were cited over 80 times in British media before Twitter identified and removed them.

Not related to Brexit but in general, most of the troll factory's Twitter activity focused on English and Russian language posts. Less than 100 000 tweets were published in German. Meanwhile, ahead of the German federal elections in September 2017, IRA accounts boosted their German messaging supporting AfD, only to slow down again after election day.

Reactions: Social Media Companies vs. Governments

INTERNATIONAL AUDIENCES FIRST LEARNED ABOUT THE TROLL FACTORY FROM RUSSIAN INVESTIGATIVE JOURNALISTS WHO EXPOSED THE OPERATION IN 2013.

Activist and investigator Lyudmila Savchuk spent two months undercover in the St. Petersburg troll factory in late 2014, and later won a lawsuit against the troll farm in 2016. She has explained the operations of her former employer in numerous publications and served as a witness in another ex-troll's lawsuit. Further details were provided by other previous trolls.

Since then, three indictments (1, 2, 3) prepared by US Special Counsel Robert

Mueller, as part of his investigation into Russian interference in the 2016 election, as well as two extensive reports by the Oxford Project on Computational Propaganda and New Knowledge, based on data provided by tech companies to the US Senate Select Committee on Intelligence (SSCI), have further refined our understanding of the troll factory's activities and operational model.

Since the enormous fallout from the 2016 US election, Twitter has **shut down and released data on nine million IRA tweets**. A searchable archive for analysts, journalists, and the general public is available here. Meanwhile, Facebook has taken down the core group of US-related IRA accounts that, in total, had almost 31 million shares, 39 million likes, and 5.4 million emoji reactions.

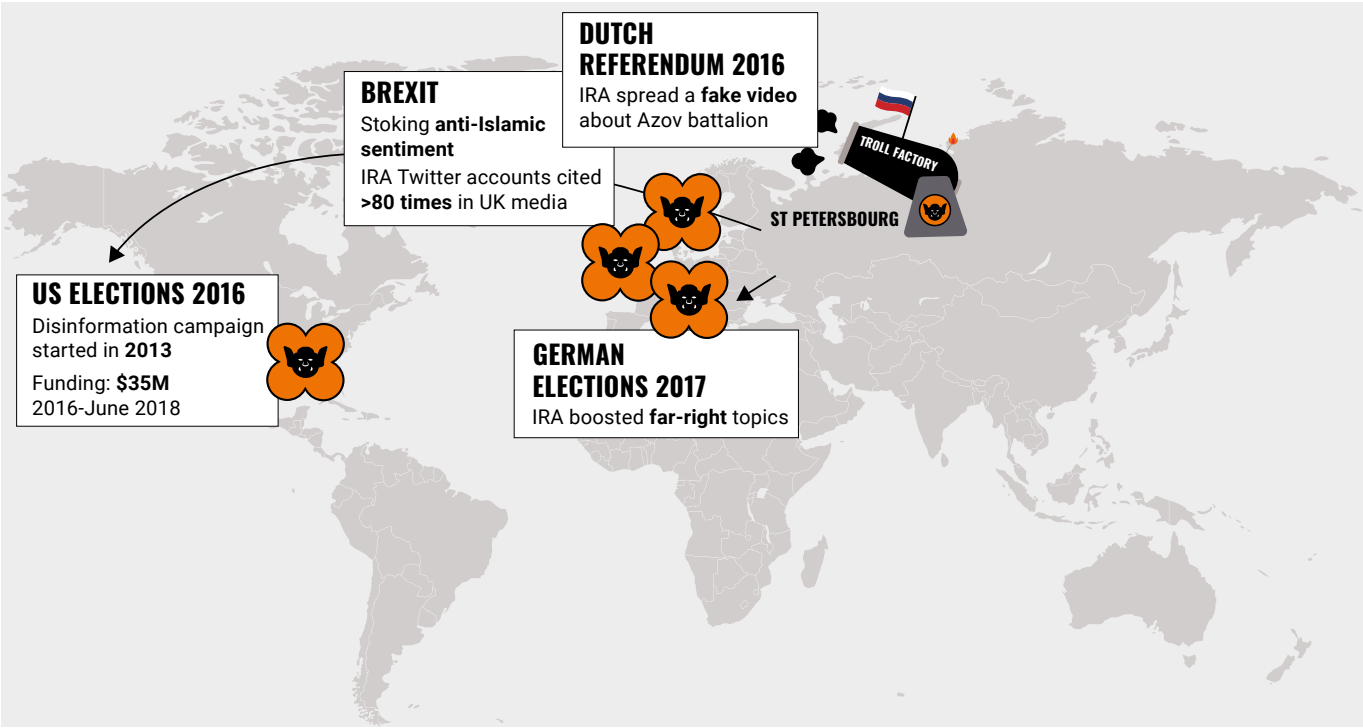
Most recently, reports have surfaced that the US military conducted its first offensive cyber-operation against the troll factory during the 2018 midterms election and blocked the IRA's internet access.

The social media companies are also facing pressure from governments and the EU to diminish their role as channels to amplify and spread disinformation. The platforms have committed to the Code of Practise, to increase transparency for political advertising and reduce the number of fake accounts. Follow monthly reporting by social media companies ahead of the European elections 2019 and Commission's responses here.

However, even though the general public can now understand the scope of Russia's online election manipulation and the sophistication of its past operations, experts remind us that the data we currently have available only provides a historical account of the IRA's tactics, but not its future ones.

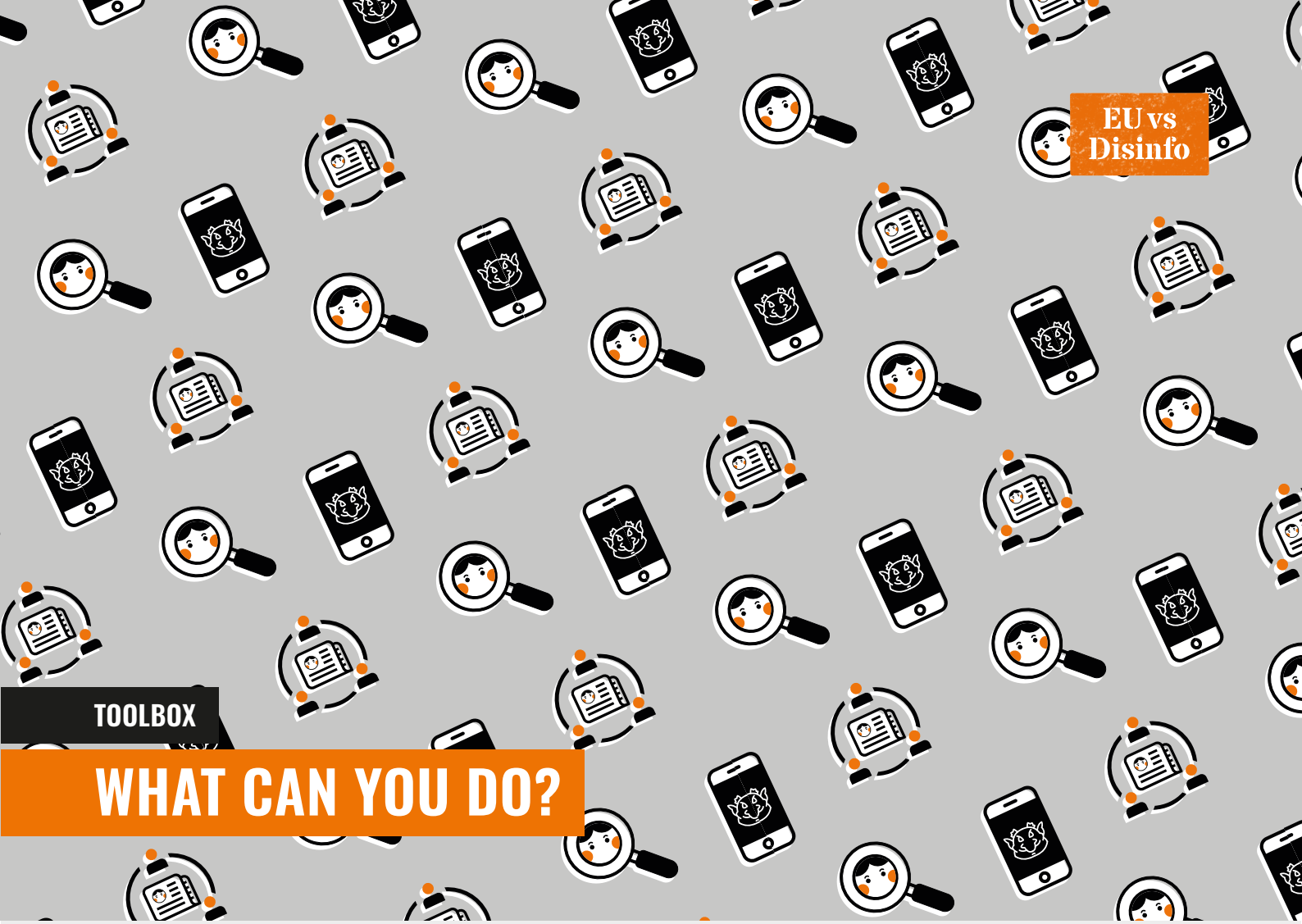
Indeed, as social media companies like Facebook and Twitter attempt to crack down on inauthentic coordinated behaviour, bad actors – both Kremlin-linked and others – are simultaneously developing innovative ways to circumvent these protections.

New tricks may include shifting strategies from the creation of disinformation to content amplification via phony social media accounts, according to experts. One emerging hacking method, for example, is breaking in to computing devices and using them to open large numbers of social media accounts at once that appear to belong to legitimate users.



Sources and Further Reading

- https://euvsdisinfo.eu/fuel-hysteria-sow-discord-spread-confusion-detailed-account-on-manipulation-attempts-before-us-elections/
- https://euvsdisinfo.eu/military-intelligence-fake-online-personas-fake-local-news-how-russia-targeted-us-elections/
- https://euvsdisinfo.eu/commanding-the-trolls/
- https://comprop.oii.ox.ac.uk/research/ira-political-polarization/
- https://www.newknowledge.com/articles/the-disinformation-report/



TOOLBOX

WHAT CAN YOU DO?

DISINFORMATION IS A BROAD, COMPLICATED PHENOMENON, WITH MANY TRICKS UPON ITS SLEEVE. NOBODY IS IMMUNE TO IT – BUT EVEN THOUGH THERE ARE NO VACCINES, THERE ARE WAYS TO BECOME MORE AWARE AND RESILIENT.

☑ Check the Content

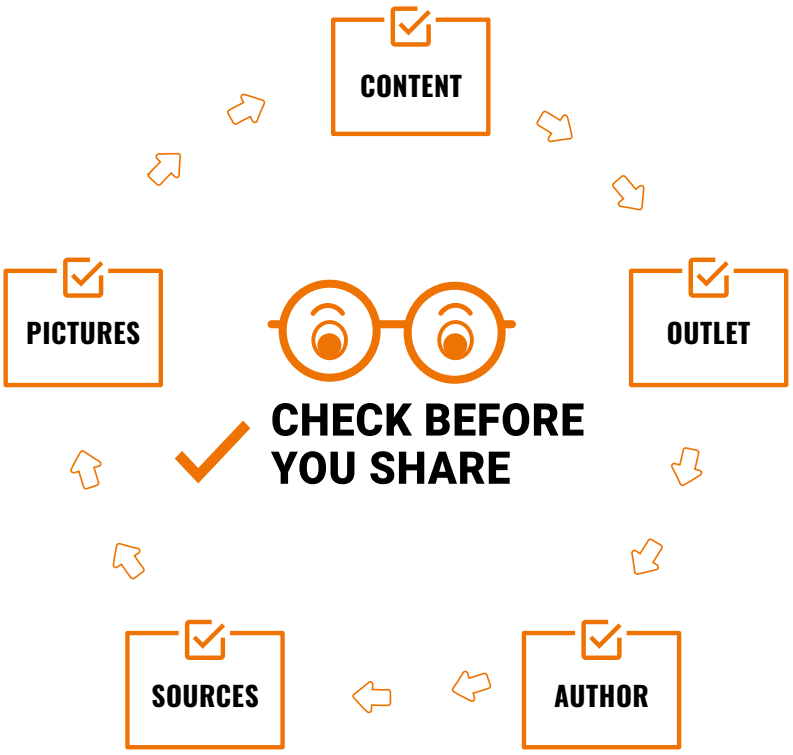
➜ News is boring. Except on rare occasions, for example when two guys rescued a dog from icy water and it turned out to be a wolf. But while the story about altar boys putting marijuana in a censer is funny, it's also a fake.

➜ If the article you are reading comes from an unknown source, check its content against well-known newspapers. Sometimes webpages of governments or NGOs can also help. Random social media accounts do not count as a reliable source.

➜ Credible media outlets have defined standards: a news piece must have more than one source and therefore, a comment offering an alternative view should be included. Look for that in articles you read.

➜ Credible media keep one-sided opinions where they belong: in the op-eds.

➜ Look at a few warning signs, used by pro-Kremlin disinformation outlets and those who relay them:



Whataboutism: An attempt to change the subject by redirecting attention. "*Sure, Russia's presence in Ukraine may be problematic, but it's no worse than what the US has done in Iraq, Libya and Syria!*"

"Trust me, I'm smart!": Facts are not dependent on a narrator's intelligence. Unfounded claims are still unfounded, no matter how clever their claimant appears to be. If someone tells you to trust them (just) because they're smart, that's probably a very good reason not to trust them.

The truth is somewhere in the middle and cannot be known for certain: While it may be true in some cases, it is often misused to obscure obvious truths. Remember: sometimes, the truth is black and white, and blame falls squarely on one side. Are Russian soldiers fighting in eastern Ukraine? Did Russian buk shoot down Flight MH17? The answer to both is yes, not "maybe, but…"

Kremlin whitewashers: Someone who is sympathetic to the Kremlin and seeks to justify or excuse its bad behaviour at all costs, typically by blaming the West for alienating Russia and destroying the relationship. "*Russia's 'aggression' is simply a response to Western neoimperialism and the expansion of NATO!*"

The Conspiracy: You've heard it before: "*Don't be naïve; the Deep State/the Establishment/the Corporations/the Jews/the Gay Lobby rules the world!*" 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!

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 2. Russia is still fighting that war to keep its own glory alive, and sees mythical fascists at every turn. Yes, everywhere. "*In reality, Ukraine/the Baltics/the White House/the US is run by fascists.*"

➜ If you want to know more, take a look at typical *pro-Kremlin narratives*.

☑ Check the outlet

➜ Do you know this outlet? If it only looks similar to a well-known medium, but is not quite the same, it can be a warning sign. Do the website name and URL look strange?

➜ Does the outlet have a significant presence in the EUvsDisinfo database?

☑ Check the Author

➜ Do you know the author and his or her previous work? A well-respected journalist always has a track record. Does this person even exist?

➜ If nobody is signed under a news piece, it should make you cautious.

➜ Beware of bots! If you see posts from very active profiles on social media (who posts 200 times a day on Twitter?), you should become suspicious. Especially if the authors are having language/syntax troubles and they have problems engaging in a real conversation on social media.

➜ According to a recent study, bots created 46% of Russian-language messaging about the NATO presence in the Baltics and Poland. The main topic of the tweets were mishaps that happened during NATO exercises.

➜ Disinforming outlets, when called upon, are often using reverse logic and may try to convince you that it is not them, but you who are confusing or disinforming the others.

☑ Check the Sources

➜ Sometimes an expert is not really an expert, but more like an "expert", specializing for example in deep state and ancient aliens. And foreign policy.

➜ And sometimes think-tanks that promise to spread progressive ideas and critical thought are just good old pro-Kremlin.

➜ If a story uses only anonymous sources or no sources at all, it should make you cautious.

☑ Check the Pictures

➜ Seeing is not believing anymore. Sometimes old images are used in new context or they are faked. Ever heard about deepfakes? Check these stories by The Wall Street Journal and The New York Times.

➜ You can try to test the picture with Google Reverse Image Search or TinEye.

☑ Think Before you Share

➜ Sometimes a great headline does not reflect the story itself. Read the article before sharing! Jokes and satire have their own ways of expression and don't have to be factual. This is why they are jokes or satire. Have a laugh and don't treat them as the truth revealed.

Have a Look What Myth-busters Are up to These Days

- https://www.bellingcat.com/
- https://blogs.ec.europa.eu/ECintheUK/euromyths-a-z-index/
- https://euvsdisinfo.eu/
- https://epthinktank.eu/tag/disinformation/
- https://ifcncodeofprinciples.poynter.org/signatories
- https://medium.com/dfrlab
- https://www.polygraph.info/
- https://www.stopfake.org/en/news/

If you need more information, check our reading list.

And if you feel like you know everything we wrote here and more,
share your knowledge with the others!