KCS Group Europe

The Growing Threat of Disinformation in Europe

October 2024

Disinformation - the distribution of misleading information used to coerce - has become a critical threat to Europe. Unlike misinformation, which is commonly shared unintentionally, disinformation is specifically crafted to disrupt stability, undermine confidence and steer public opinion. In recent years, Europe has become a hotspot for such campaigns, with prominent states like Russia utilising sophisticated tactics to influence everything from elections to economies. These actions take advantage of existing differences and divisions and use social media to drive a wedge into sensitive political issues, causing confusion and unrest with a view to destabilise.

Defending against disinformation is a pressing concern, particularly in the case of Russia's war with Ukraine, where campaigns are launched by the Kremlin at an unprecedented scale. Referred to as hybrid warfare - military actions combined with disinformation, cyber-attacks, economic coercion and other non-military tools - this strategy is aimed at destabilising Ukraine and broader democratic institutions across Europe. The European Union (EU) has sought to respond by improving its capabilities to identify and counter threats, as seen in initiatives like the EU vs Disinfo platform, which has been tracking over 5,500 disinformation cases about Ukraine since 2015.

The implications for multinational corporations are profound. Disinformation can redirect market perceptions, influence policies and provoke regulatory backlash that can seriously impact operations across the continent. For decision-makers, understanding the tools, methods and impacts of disinformation is vital for safeguarding against these threats. Identifying and mitigating the risks associated with disinformation is now a recognised core element of risk management strategy.

Strategic relevance: disinformation's impact on Europe

These nefarious campaigns are contributing to an already eroding public trust in Europe, which is breaking social unity, making them a serious concern for businesses. Often state-sponsored, disinformation attacks political stability by influencing opinions and policymaking, which creates unpredictable conditions. For business, this heightens operational risk planning, compliance and market perception.

The EU is aware of the risks. Despite efforts, like the Stratcom team within the European External Action Service, the EU is confronted by significant challenges in countering Russian interference. Efforts are further complicated by a fragmented and mostly under-resourced response network across member states, making the region vulnerable to disinformation operations that prey on grievances and support nationalist narratives.

The mechanisms of disinformation: tactics and tools

Hybrid warfare is sophisticated, employing a variety of strategies to manipulate opinion and destabilise. False narratives are spread across social media, forums, news outlets and other online platforms. These threads are then amplified by manipulated algorithms, ensuring content spreads far and wide quickly. Deepfakes allow for convincing video manipulation, and bots and troll farms both create and distribute disinformation at an alarming scale, challenging the public to recognise the truth from fabrication.

Disinformation from the Kremlin involves leveraging multiple channels to reach various audiences. For example, in Central and Eastern Europe, where social media platforms like X are not so prevalent, disinformation is fed through local-language outlets, emails and direct messaging platforms like Teams, Zoom, WhatsApp, Messenger or Signal. The goal is not only to get false information out there but also to cause mistrust in institutions and amplify existing divisions.

It is important to understand that these attacks are not random, they are designed specifically to exploit sensitive issues and influence public opinion in ways that serve the interests of those orchestrating the campaigns.

Case studies: disinformation impacting key European countries

Russia's influence in European elections illustrates how disinformation can alter the outcomes of democratic processes.

In the 2017 French presidential election, disinformation campaigns attacked Emmanual Macron by using "Macron Leaks" the huge data dump released just days leading up to the final vote. The leak consisted of a blend of genuine and fabricated content, believed to be controlled by Russian state sponsored group APT28 looking to discredit Macron.

The 2021 German federal election saw the sharp end of disinformation effects, with a much broader scope than was seen in France. Key to these various campaigns was the spread of misleading data regarding COVID-19, which included vaccines and lockdown measures looking to undermine public confidence in the government and influence voter opinions. Several candidates like the Green Party's Annalena Baerbock, were subjected to co-ordinated attacks involving fabricated narratives about their personal lives and political positions aimed at reducing their public appeal. There was believed to be Russian involvement following the surfacing of far-right agendas that were supported by legions of conspiracy theorists and Russian state-controlled media such as RT and Sputnik. German authorities and cybersecurity agencies did all they could to protect the integrity of the elections and unprecedented distribution of fake news.

Leading up to the 2024 European Parliament elections, disinformation gained momentum, as was seen in countries like Poland, Germany and France. The content singled out mainstream parties and leaned on voter grievances, providing support for nationalist administrations. The EU's efforts to defend against these intrusions had been marred by a lack of resources and co-ordinated strategies among states.

These campaigns do not stop at politics but also target industry. In the energy sector, disinformation has manipulated perceptions surrounding energy policies and climate initiatives, causing confusion and delaying policy change. The finance sector has been subjected to false narratives that have gone on to disrupt markets and erode confidence in forecasts. Tech companies are now facing challenges as they become both targets and unwilling disseminators of disinformation, affecting strategies and ethical responsibilities.

Protecting corporate interests in a disinformation-prone environment

To protect corporate interests in a world saturated with disinformation, businesses must form a proactive and strategic approach. Developing comprehensive disinformation risk strategies is essential. This should include crisis management protocols that can be engaged quickly when nefarious campaigns surface.

Fostering a work culture of openness and factual integrity in corporate communications is imperative. Monitoring and validating internal and external communication streams will ensure that information is grounded and verified. Incorporating disinformation risk into wider risk management approaches is now a necessity. By embedding this awareness into corporate culture, firms can start to protect their reputations and operational capabilities in this rapidly evolving information age.

Conclusion: confronting disinformation in Europe – a corporate imperative

The threat of disinformation in Europe is significant to both political stability and corporate integrity. Campaigns that form part of a grander hybrid warfare strategy are not just designed to distribute falsehoods, they also aim to manipulate market perceptions and destabilise societies. For the multinational, the risk is clear: if you do not acknowledge and mitigate this threat, it could lead to fatal operational disruption, reputational damage and strategic mistakes.

Decision-making executives need to recognise the urgency of combating disinformation. By integrating disinformation risk into corporate risk management frameworks, corporations can protect their interests and reputation. Act now before these targeted campaigns become an even more menacing force in Europe.