

FOREIGN INFORMATION MANIPULATION AND INTERFERENCE – CREATING A COMMON BASIS FOR ACTION

The European Democracy Action Plan (EDAP) set out a distinction of the different phenomena that are commonly referred to as ‘disinformation’. Despite the differentiation already included in the EDAP, there is a clear need for further work towards more refined common definitions and methodologies. Regarding one of these phenomena – the activities of foreign actors – the EEAS has started to review and bring together in one coherent approach and common understanding the different elements with a view to operationalising their use which will enable future possible coordinated or joint responses. In this context, it is suggest to use the term “foreign information manipulation and interference”, rather than “disinformation”, as it more accurately captures the issue at stake.

Any response requires a sound and robust shared situational awareness and a clear understanding of the type of behaviour that the EU wants to deter and respond to, i.e. what should be considered impermissible manipulative behaviour¹. To establish such a shared situational awareness, the EU has increased its cooperation with civil society and industry, but also through information sharing between the EU institutions and the Member States, notably via the Rapid Alert System (RAS).

However, a more granular practical and inter-operational framework is necessary to allow for the development of a common methodology within the EU and potentially with other stakeholders² to gain shared situational awareness, conduct systematic evidence collection and detection of manipulation of the information environment.

Concretely, shared situational awareness and an updated definition need to capture the tactics, techniques and procedures (TTPs) that describe the patterns of behaviour of the threat actor. To this day, different stakeholders are operating with different definitions– social media platforms, civil society, governments all have their own concept that describes the challenge (e.g. “disinformation”, “coordinated inauthentic behaviour”, “information operations”).

A BASIS FOR A CONCEPTUAL DEFINITION

The building blocks proposed in this paper aim to capture what should be the basis for the shared understanding and a conceptual framework of the manipulation of the information environment.

Only a combination of these elements will constitute what we consider illegitimate behaviour in the information environment.

- **Grey zone activity:** While terrorist content and hate speech, for example, are clearly defined as illegal, foreign information manipulation and interference is deliberately using the grey zone of the “non-illegal” space. Foreign information manipulation and interference sometimes can occur in coordination with illegal behaviour, such as non-illegal foreign information manipulation and interference following an illegal hack-and-leak operation in the cyber domain.

- **Values, procedures and political processes:** Foreign information manipulation and interference has the potential to negatively impact fundamental rights and freedoms as

¹ See also 6.1 of the Guidance on Strengthening the Code of Practice on Disinformation (COM(2021) 262 final).

² This could be international like-minded partners, such as G7, NATO, but also civil society organisations, academia, research organisations and industry.

well as the values that the European Union has been founded upon, as enshrined in Art. 2 of the Treaty on the European Union. Such goods are human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. Public goods can further be broken down accordingly, such as the protection of free and fair elections, freedom of expression, etc. An assessment of how, with which aim and in which intensity these goods are being threatened, i.e. the determination of the threat level, is necessary.

- **Manipulation:** The activity described as foreign information manipulation and interference is distinct from organic and authentic patterns of behaviour. The identification and collection of TTPs is a key element in establishing the criterion of manipulation; it can include diverse elements like the manipulation of facts (e.g. the spread of false/misleading information), the use of fake social media accounts, setting up of fake websites, forged letters, censorship of critical/independent voices, online harassment, etc. All of these activities manipulate the information environment, giving a distorted impression of public opinion and of reality.
- **Intentional:** Proving intent to manipulate the information environment is one of the key challenges, but also one of the key elements for identifying foreign information manipulation and interference. In this regard, the combination of different TTPs as well as their repeated use by a threat actor will help to establish an intent to manipulate the information environment.
- **Coordinated:** Foreign information manipulation and interference describes a pattern of behaviour and includes therefore an element of coordination, i.e. the combination of different TTPs to enable them to work together effectively. It also accounts for the broader ecosystem that has evolved by including the ability to use different parts of this ecosystem, e.g. the use of government officials together with state-sponsored media outlets and state-controlled organisations.
- **State or non-state actors** and/or their **proxies:** Foreign information manipulation and interference can be conducted by foreign governments or by foreign non-state actors themselves, including elements that are directly and publicly linked, financed and controlled by them. However, foreign information manipulation and interference can also include the use of so-called proxies, where no direct link is publicly established, but where such elements are linked, financed and controlled in a covert manner.

Given the above, a suitable definition of the threat could be captured with the following concept:

“Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.”