BRIEFING
STOA Options Brief

European Parliament

Strategic communications as a key factor in countering hybrid threats

Hybrid threats, a dangerous phenomenon for democratic societies

The concept of a **hybrid threat** synthesises a **complex and evolving phenomenon**, where state and non-state actors use diverse tools to influence different forms of decision-making, undermine citizens' trust in democratic processes and institutions, exacerbate political polarisation, spread confusion about geopolitical events and weaken legitimate governments, with the ultimate goal of destabilising the victim. The use of digital technologies constitutes a differential and key component of modern hybrid threats, as it exacerbates its potential damage.

Hybrid threats encompass a wide range of means and tools: disinformation campaigns, cyber-attacks, espionage, promotion of irregular migration, manipulation of international law, deployment of irregular armed groups and conventional forces, as well as political subversion and propaganda, religious influence, sabotage, terrorism, economic pressure and energy dependence.

Hybrid threats can be countered by developing measures in different fields (political and diplomatic, informative, economic, intelligence, legal and military) and at different times (preventive, detection and response measures).

Strategic communications as response to hybrid threats

Strategic communications are a key element to counter the components of hybrid threats in the information field. They are defined as 'Systematic series of sustained and coherent activity, conducted across strategic, operational and tactical levels; that enables understanding of target audiences, identifies effective conduits, and develops and promotes ideas and opinions through those conduits to promote and sustain particular types of behaviour'.[1] They are executed according to: a predetermined and systematic plan; imply actions at strategic, operational and tactical levels; demand a high level of coordination and synchronisation between agents; require the accurate definition of target audiences; require selection of the most appropriate communications channels; are aimed not only at informing but also at influencing and promoting behavioural changes in target audiences; must be aligned with the overall objectives of the promoter; and must focus on both the short and the long term.

Digital technologies have great impact on strategic communications, creating new opportunities to both spread messages to large audiences in a rapid and inexpensive way and define customised narratives for very specific groups.

The protection of information is an essential prerequisite to control communications. Therefore, telecommunications networks security is one of the main pillars for the success of strategic communications. This is why security of the new 5G networks has become a salient issue in recent

times. Artificial intelligence (AI) plays a double role here, as it can be used by both the promoters of hybrid threats to develop more sophisticated attacks and by defenders to counter them. AI can be used to create and spread false content (text, images, audios, videos) without human intervention, which could accelerate and reduce the costs of disinformation campaigns. It is also a key technology used in detecting and preventing disinformation and other components of hybrid threats. Other technological innovations, such as the Internet of Things (IoT) and blockchain, contribute to improved strategic communications. While IoT allows a high volume of data and information to be collected to better understand what is happening before defining a communication strategy, blockchain helps to ensure the integrity and veracity of information and to detect disinformation more quickly.

Challenges to effectively counter hybrid threats in the EU

The European Union (EU) has already implemented different measures to counter hybrid threats. However, vulnerabilities, and the challenges they represent, persist.

The protection of European institutions and citizens against hybrid threats requires a harmonised legal and regulatory framework, which must be the foundation of all policies and actions to deal with this phenomenon. The success of the measures to face hybrid threats heavily depends on the identification of perpetrators, while the growing technological sophistication of attacks and the use of digital channels make this identification very complex. Social media platforms have become one of the main channels for spreading disinformation. However, digital service providers are still playing a very tepid role in the fight against this type of hybrid threat. One of the objectives of hybrid threats, especially disinformation campaigns, is to hamper the ability of citizens to take informed decisions. EU citizens' lack of awareness of disinformation contributes to its success. The EU has developed a wide network of units, teams, agencies and other advisory bodies to fight hybrid threats and, particularly, disinformation. However, a better coordinated response is still lacking, as each body usually addresses this issue in an isolated manner. The EU is highly dependent on foreign providers in very sensitive areas, such as cyber-intelligence, cybersecurity, 5G infrastructure or AI. This may make it difficult to counter hybrid threats while respecting EU values and principles. It also entails the risk of leaving very sensitive information, which could be misused against the EU's interests, in third party hands. The EU should adopt more proactive approaches to combat disinformation, leveraging strategic communications to anticipate the malicious actions of hybrid threat promoters and limit their effects.

Policy options

The complex phenomenon of hybrid threats can be addressed from many different perspectives. For this reason, the study describes and assesses a broad set of policy options. They are organised in the following eight categories.

Policies related to regulation against hybrid threats

- Development of the European strategy against hybrid threats, disinformation and foreign interference (EU-HTDFI strategy). This strategy would be the basis for the further implementation of specific legal instruments.
- Regulation of risks analysis for hybrid threats. Conducting risk analysis to counteract hybrid threats should be mandatory for Member States and legally regulated at the EU level.
- Harmonisation of the EU legal framework against hybrid threats, disinformation and foreign interference.
- Adaptation of a sanctions regime to be used against promoters of hybrid threats, disinformation and foreign interference.
- Updating of the Cybercrime Convention Committee (T-CY) interpretation of interference in electoral processes. The lack of truthfulness in such information should be incorporated as an element that can constitute a crime.

- Improvement of AI regulation to ensure the correct use of this technology by public authorities; to prevent, detect and respond to hybrid threats, disinformation and foreign interference.

Policies related to attribution of hybrid threats

- Increase economic resources allocated to the attribution of threats.
- Increase economic resources allocated to the detection of disinformation.

Policies related to the role of social media platforms in the fight against hybrid threats

- The Code of Practice on Disinformation for social media platforms operating in the EU should become mandatory, adding periodical external audits.

Policies aimed at raising awareness about hybrid threats

- Incorporation of critical information analysis competences in the school curriculum to increase critical thinking skills and media literacy among children and young people.
- Introduction of teacher training and ongoing development of educative resources and contents. This is a prerequisite to improve critical thinking skills among citizens, particularly young people.
- Introduction of policy-maker training. Policy-makers should lead the fight against disinformation, and therefore require the necessary skills and tools.
- Introduction of digital literacy programmes for people with low digital competence. An effective way to combat disinformation is to enhance digital literacy among EU citizens, particularly those with low digital competences.
- Promotion of citizens' guides for detecting disinformation. The development of informative guides to help detect disinformation would increase awareness about this threat.

Policies related to coordination and information sharing between stakeholders

- Creation of a coordination unit at the EU level to unify responses against hybrid threats.
- Creation of common response mechanisms at the EU level. Although the response to hybrid threats is mainly a national competence, the EU should urge Member States to adopt harmonised mechanisms to fight hybrid threats homogeneously.
- Intensify cooperation between the EU and NATO, which is essential considering the practical measures necessary to prevent, detect and respond to hybrid threats.
- Development of training exercises on countering hybrid threats, involving all stakeholders.
- Increase in operational intelligence capability at the EU level, developing an EU intelligence agency.
- Development of a European cyber-surveillance tool (ECT) to facilitate EU institution and Member State' monitoring of cyberspace to detect and prevent hybrid threats.
- Increase in public-private cooperation: telecommunication operators, cybersecurity firms, media outlets, social media platforms, utilities and financial companies are all key agents in the fight against hybrid threats and public authorities should define new ways to collaborate with them.

Policies related to the digital technology gap between the EU and its competitors

- Increase in research and development investments and financial support for start-ups and scale up companies related to digital technologies.
- Development of industrial policies for key technologies (5G, AI, IoT, Blockchain).

Policies aimed at supporting the use of digital channels to fight hybrid threats

- Allow public authorities to exceptionally intervene in digital services to fight hybrid threats.
- Improve law enforcement in 5G networks. Lawful interception of communications may be more difficult in 5G networks, hindering police work. The EU should promote the development of tools that help to overcome this issue.

Policies aimed at defining proactive approaches to deal with hybrid threats

- Strengthen the EU vision and values outside the EU borders.
- Support free journalism against disinformation in vulnerable countries.
- Mandatory creation of Strategic Communications units (StratCom) at the highest level in EU countries and institutions.
- Creation of an EU news agency to ensure the veracity of information.
- Improve diplomatic relations with countries considered as strategic challenges for EU security.

ENDNOTE

[1] Tatham, S., Strategic Communications: A Primer. *ARAG Special Series, Defence Academy of the United Kingdom*, 8(28), 2008, pp 3.

This document is based on the STOA study 'Strategic communications as a key factor in countering hybrid threats' (PE 656.323) published in March 2021. The study was written by Juan Pablo Villar, Carlota Tarín, Julio Blázquez (Iclaves S.L.), Carlos Galán Pascual (Carlos III University) and Carlos Galán Cordero (Universitat Oberta de Catalunya) at the request of the Panel for the Future of Science and Technology (STOA), and managed by the Scientific Foresight Unit, within the Directorate General for Parliamentary Research Services (EPRS), European Parliament. STOA administrator responsible: Zsolt Pataki

DISCLAIMER AND COPYRIGHT

stoa@ep.europa.eu (contact)

http://www.europarl.europa.eu/stoa/ (STOA website)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)