Strategic communications as a key factor in countering hybrid threats

STUDY

Panel for the Future of Science and Technology

EPRS | European Parliamentary Research Service

Scientific Foresight Unit (STOA)

PE 656.323 – March 2021

EN

Strategic communications as a key factor in countering hybrid threats

This report describes the key features, technologies and processes used in strategic communications to counter hybrid threats and their components.

A theoretical description of hybrid threats is complemented by an analysis of diverse case studies, describing the geopolitical context in which the hybrid threat took place, its main features, the mechanisms related to strategic communications used by the victim to counter the hybrid threat and its impact and consequences.

A comprehensive set of policy options aimed at improving the EU response to hybrid threats is also provided.

AUTHORS

This study has been written by Juan Pablo Villar García, Carlota Tarín Quirós and Julio Blázquez Soria of Iclaves S.L., Carlos Galán Pascual of the University Carlos III of Madrid, and Carlos Galán Cordero of the 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) of the Secretariat of the European Parliament.

ADMINISTRATOR RESPONSIBLE

Zsolt Pataki, Scientific Foresight Unit (STOA)

To contact the publisher, please e-mail stoa@ep.europa.eu

LINGUISTIC VERSION

Original: EN

Manuscript completed in March 2021.

PE 656.323
ISBN: 978-92-846-7812-9
doi: 10.2861/14410
QA-02-21-202-EN-N

http://www.europarl.europa.eu/stoa (STOA website)
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

The hybrid threat concept and its components

The hybrid threat concept attempts to synthesise a complex and evolving phenomenon, where state and non-state actors use diverse means and tools to influence different forms of decision-making, undermine citizens' trust in democratic processes and institutions, exacerbate political polarisation and spread confusion about geopolitical events with the ultimate goal of destabilising the victim while reinforcing the political vision and values of the offender. The use of digital technologies constitutes a differential and key component of modern hybrid threats, as it exacerbates their potential.

Hybrid threats can be characterised as follows:

- They are coordinated and synchronised;
- deliberately target democratic states' and institutions' systemic vulnerabilities;
- use a wide range of means;
- exploit the thresholds of detection and attribution as well as different interfaces (war-peace, internal-external, local-state, national-international, friend-enemy);
- aim to influence different forms of decision-making at the local, state, or institutional level;
- favour and/or achieve the agent's strategic goals;
- while undermining and/or hurting the target.

Promoters of hybrid threats can use a wide range of actions to achieve their goals. This study analyses these components related to strategic communications and digital technologies: (1) funding organisations and political parties for propaganda, (2) strategic leaks and cybertools, (3) social media and domestic media outlets, (4) paramilitary organisations, (5) religious influence, (6) economic pressure and (7) concerns about migration.

Disinformation campaigns play a crucial role in hybrid threats

Disinformation is a key component of hybrid threats. It can be defined as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public'. Disinformation campaigns take advantage of the possibilities opened up by digital platforms.

Responses to hybrid threats: the role of strategic communications

Responses have been categorised according to two dimensions: action areas and the time frame in which the action should be taken. Action areas encompass (1) political or diplomatic actions, (2) informative actions, (3) economic of financial actions, (4) intelligence actions, (5) legal actions and (6) military actions. Regarding the time frame, actions are categorised as (1) preventive measures, (2) detection measures and (3) response measures. Some of these measures are considered within the scope of strategic communications. Strategic communications may, for the purposes of this study, be defined as the 'systematic series of sustained and coherent activities, 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' (Tatham, S., 2008, p. 3).

The essential characteristics of strategic communications can be summarised as follows:

- They are executed according to a predefined and systematic plan;

- involve actions at strategic, operational and tactical levels;
- are developed in a competitive, and even conflictive, environment, where audiences are subject to a constant buzz that can hamper their goals being met;
- demand a high level of coordination and synchronisation between stakeholders;
- require targeted audiences to be exactly defined;
- require selection of the most adequate communication channels;
- are aimed at informing, influencing or promoting behavioural changes in the target audiences;
- must be aligned with the overall goals of the promoter country or organisation;
- must be focused on both the short and long term.

Digital technologies have a relevant impact on strategic communications

Digital technologies open up great opportunities to spread messages amongst broad audiences in a rapid and inexpensive way, and to create customised narratives for specific audiences. Digital technologies can be used by both promoter of hybrid threats to fabricate and spread disinformation, and the institutions that fight them to develop counter-narratives.

The 5G standard represents a quantum leap in the field of communication infrastructure, which is bound to revolutionise strategic sectors. Telecommunication network security is critical to countering hybrid threats.

Other relevant technological innovations that can act as a driver for the development of hybrid threats are (1) artificial intelligence (AI), (2) the Internet of Things (IoT) and (3) blockchain technologies.

From theoretical analysis to practical implementations of hybrid threats and the use of strategic communications to counter them

Seven practical implementations of hybrid threats across the world are analysed:

- the most paradigmatic case of hybrid threat: the Russian attacks against Ukraine that led to the illegal annexation of Crimea;
- four cases that include new or enhanced hybrid attack mechanisms and/or innovative strategic communications measures in the response: support for the Salafi movement in the Netherlands by the Gulf monarchies; Saudi Arabian pressure on Pakistan regarding the civil war in Yemen; foreign influence of Russia and China through academic institutions and think tanks; and Russian electronic warfare during the Zapad 2017 exercises;
- two recent cases that have drawn the attention of policy-makers and analysts: disinformation campaigns against NATO operations in Lithuania, and disinformation attacks in the Catalan issue.

Altogether, these cases, reflect all the components and essential characteristics of hybrid threats, and the responses include interesting insights into the field of strategic communications.

Successful responses that use communication strategies share common characteristics: proactivity by implementing preventive measures, such as awareness campaigns, intense cooperation amongst stakeholders and an elaborate, coherent and solid narrative.

Case studies show that strategic communications have a great potential to counter hybrid threats. However, more proactive approaches, better cooperation and more intensive use of digital technologies are needed to provide more efficient and effective responses to hybrid threats.

Policy options to tackle hybrid threats

Although the EU has already implemented different measures to counter hybrid threats, vulnerabilities persist. The policy options proposed in this study are aimed at facing hybrid threats by addressing such vulnerabilities. They have been grouped into eight categories:

- Policies related to regulation against hybrid threats.
- Polices related to attribution of hybrid threats.
- Policies related to the role of social media platforms in the fight against hybrid threats.
- Policies aimed at raising awareness about hybrid threats.
- Policies related to coordination and information sharing between stakeholders.
- Policies related to the digital technology gap between the EU and its competitors.
- Policies aimed at supporting the use of digital channels to fight against hybrid threats.
- Policies aimed at defining proactive approaches to dealing with hybrid threats.

Table of contents

List of figures

List of tables

List of abbreviations

AAUP	American Association of University Professors
AI	Artificial Intelligence
APT	Advanced Persistent Threat
AQAP	Al Qaeda in the Arabian Peninsula
CAUT	Canadian Association of University Teachers
CEC	Central Election Commission
CERT	Computer Emergency Response Team
CFI	Counter Foreign Interference
CFSP	Common Foreign and Security Policy
CI	Confucius Institute
CIS	Commonwealth of Independent States
CoE	Centre of Excellence
COP	Conference of the Parties
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
DCCC	Democratic Congressional Campaign Committee
DDoS	Distributed Denial of Service
DNC	Democratic National Committee
EACS	European Association for Chinese Studies
ECT	European Cybersurveillance Tool
EFP	Enhanced Forward Presence
EIB	European Investment Bank
eIDAS	electronic Identification, Authentication and trust Services
EU-CHTC	EU Counter Hybrid Threat Coordinator
EUAM	European Union Advisory Mission
FPI	Foreign Policy Instruments
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GONGO	Governmental-Organised Non-Governmental Organisation
HTDFI	Hybrid Threats, Disinformation and Foreign Interference
ICAS	Institute for China-American Studies
IDC	Institute of Democracy and Cooperation
IEA	International Energy Agency

IGO	Intergovernmental Organisation
INTCEN	Intelligence Analysis and Situation Centre
IT	Information Technologies
IOP	Instruments of Power
IoT	Internet of Things
JIT	Joint Investigation Team
MS	Member State
NATO	North Atlantic Treaty Organisation
NCFIC	National Counter Foreign Interference Coordinator
NGO	Non-Governmental Organisation
NIS	Network and Information Security
NSS	National Security Strategy
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the High Commissioner for Human Rights
OSCE	Organisation for Security and Co-operation in Europe
OSINT	Open Source Intelligence Sources
PACE	Parallel And Coordinated Exercises
RICU	Research and Information Communication Unit
ROC	Russian Orthodox Church
RT	Russia Today
R&D	Research and Development
SITE	Security Intelligent Threats to Elections
STC	Southern Transitional Council
StratCom	Strategic Communications
T-CY	Cybercrime Convention Committee
UAE	United Arab Emirates
UAV	Unmanned Aerial Vehicle
UN	United Nations
UNFCCC	United Nations Framework Convention on Climate Change
UOC	Ukrainian Orthodox Church
USSR	Union of Soviet Socialist Republics
UUV	Unmanned Underwater Vehicle

1. Introduction

In recent years, European countries, and the EU as a whole, have witnessed several attempts at destabilising society and legitimate governments. State and non-state actors, both foreign and domestic, have tried to undermine citizens' trust in democratic processes, exacerbate political polarisation and spread confusion about geopolitical events by using different strategies. These strategies, which range from disinformation campaigns to the use of migration as a pressure element, constitute what has been called 'hybrid threats'. The promoters of hybrid threats seek to weaken their adversary in an inexpensive and rapid way, without the need to use conventional means of warfare, and always remaining below the threshold of direct attribution of authorship.

Many of the strategies deployed in hybrid threats are related to the fields of information and communication. Digital technologies are of paramount importance in these areas, for both the execution of hybrid actions and for countering them. In fact, services such as social networks or video sharing platforms and technologies such as artificial intelligence play a double role in the realm of hybrid threats: they can be used as both enablers and barriers to hybrid threats. In such a scenario, one of the essential instruments to counter the effects of hybrid threats is strategic communication. For the purposes of this study, strategic communication may be defined as a 'systematic series of sustained and coherent activities, 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' (Tatham, S., 2008, p. 3) Its main goal is to provide narratives to the targeted audiences through appropriate channels in a timely way in order to prevent, detect and reduce or eliminate the consequences of hybrid threats.

Geopolitical tensions across the world are fuelling the deployment of hybrid threats and the use of strategic communications to counter them, by all kind of actors. The growing rivalry between the USA and China for world economic hegemony, ongoing overt or covert conflicts in the Middle East, Russia's desire to regain influence in the international sphere, the political instability in certain regions (Venezuela, North and Central Africa) and the rise of extremist movements at both sides of the political spectrum in Europe and North America are the main arenas where hybrid threats are arising. Most recently, the Covid-19 pandemic has emerged as a relevant factor of destabilisation for security and cooperation, even being compared to a kind of hybrid warfare (Hybrid CoE, 2020b). The Covid-19 pandemic has allowed another form of soft power exercise to flourish, promoted by China and clearly linked to the concept of strategic communication (Karnitschnig, M., 2020).

China's economic growth in recent decades has fuelled a shift in its foreign policy, turning the country's eyes abroad. Improving the country's external image is a vital objective for the Chinese government in order to increase its cultural and ideological influence, and therefore enhance its soft power. The Confucius Institute, which will be analysed as a case study in Chapter 4, is one of its most important tools. However, the Covid-19 world crisis has jeopardised any progress made in recent years. The emergence of the virus in China has threatened the country's image. In response, the country has launched a major communication strategy to debunk the accusations of mismanagement and lack of transparency at the onset of the pandemic. This strategy, although it is still too early for it to be fully assessed, includes at least three areas of action. Firstly, China made a major effort to show the world the efficiency of its management and governance and its spirit of international collaboration, especially with international health organisations. Secondly, China presented itself as an ally in helping other countries fight the virus. China sent doctors, expert teams and medical supplies to other nations such as Italy, Spain, the Netherlands, Poland, Cambodia, Iran, Iraq, etc. Finally, China engaged in an open and public 'blame game' with its main geopolitical competitor, the USA, regarding responsibility for the emergence of the coronavirus. The spokesman for the Chinese Foreign Affairs Ministry accused the US Administration of withholding information about the first cases of the virus in the United States, arguing that it was possible the virus was introduced to China by American soldiers. In response to

China, President Trump made public declarations related to the coronavirus crisis, calling it the *Chinese virus* (Gil, T., 2020).

Far from reducing the number of hybrid threats, the current international health crisis seems to be a breeding ground for their proliferation.

Within this context, this study aims to analyse the concept of hybrid threats, their components and the potential means to counter them, taking into account the perspective of digital technologies and the role that strategic communications play. Some case studies of recent hybrid threats developed across the world are presented as an introduction to the description of the challenges the EU must face to effectively tackle hybrid threats. Finally, policy options to address these challenges are assessed.

The study is structured as follows:

- Chapter 1. Analysis of hybrid threats. This chapter describes the concept of hybrid threats and their main components, with special focus on disinformation campaigns.
- Chapter 2. Strategic communications as response to hybrid threats. Chapter 2 is devoted to describing of strategic communications and its elements. It also includes a detailed analysis of the impact of digital technologies on strategic communications, as well as a summary of national and international initiatives using elements of strategic communications to combat hybrid threats.
- Chapter 3. Description of case studies. This chapter analyses seven case studies from recent years which, overall, include all the components and essential characteristics of hybrid threats and responses in the field of strategic communications.
- Chapter 4. Challenges in effectively countering hybrid threats. Based on the findings of previous chapters, Chapter 4 describes the vulnerabilities and the challenges they represent, which the EU must face to successfully manage hybrid threats.
- Chapter 5. Policy options. This chapter describes and assesses a comprehensive set of policy options aimed at improving the EU's response to hybrid threats.
- Chapter 6. Conclusions. The last chapter provides final reflections on the main findings related to the concepts analysed (mainly hybrid threats and strategic communications), the EU's current state of play to counter hybrid threats and the policy options that are most suitable for tackling them.

2. Analysis of hybrid threats

2.1. Concept and scope of hybrid threats

Defining hybrid threats

The concept of hybrid threats aims to synthesise a complex and evolving phenomenon. In recent years, diverse institutions, from the European Parliament[1] to NATO,[2] have provided different definitions. Nevertheless, the most comprehensive one, according to the experts consulted when drawing up this report, is that offered by the Hybrid CoE (the European Centre of Excellence for Countering Hybrid Threats). According to this source, the **essential characteristics** of hybrid threats are as follows (Hybrid CoE, 2020a):

- They are coordinated and synchronised;
- deliberately target the systemic vulnerabilities of democratic states'[3] and institutions;
- use a wide range of means;
- exploit the thresholds of detection and attribution as well as different interfaces (war-peace, internal-external, local-state, national-international, friend-enemy);
- aim to influence different forms of decision-making at the local (regional), state, or institutional level;
- favour and/or achieve the agent's strategic goals;
- undermine and/or hurt the target.

Both the literature reviewed and the experts interviewed agree that two of the greatest strengths of hybrid threats, which make them extremely difficult to address, are their **ambiguity** and the difficulty of **attributing** them to a particular actor (NATO StratCom CoE, 2019). Promoters of hybrid threats usually conceal their real intentions and objectives. They also try to deceive the victims about the origin of the threat, so the victims cannot adequately respond, as it is very difficult for them to identify who is really responsible.

Means and objectives of hybrid threats

As the Hybrid CoE states in the previous definition, hybrid threats are developed through a wide set of means and tools. The NATO StratCom Centre of Excellence includes the following (NATO StratCom CoE, 2019): (1) disinformation campaigns; (2) cyberattacks; (3) facilitated migration; (4) espionage; (5) manipulation of international law; (6) threats of force (by both irregular armed groups and conventional forces); (7) political subversion; (8) sabotage; (9) terrorism; (10) economic pressure; (11) energy dependency.

Hybrid threats can pursue specific objectives linked to specific situations related to the victim, for instance, getting a candidate to win an election by meddling in the electoral process through

[1] 'A phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat' (EPRS, 2015).

[2] From the point of view of NATO, hybrid threats are 'A type of threat that combines conventional, irregular and asymmetric activities in time and space', stressing that this is a threat that owes its dangerousness to the synergies generated by its various components when used in combination (Treverton, G. et al., 2018).

[3] It should be noted that our analysis has shown, nevertheless, that hybrid threats can also target non-democratic states.

disinformation. However, they are usually aimed at more strategic and long-term goals such as (Alvargonzález, A., 2018):

- Eroding citizens' trust in their institutions.
- Generating mistrust in the democratic system.
- Undermining social cohesion or social models of states, political communities (such as the EU) or international organisations (NATO, for example).
- Weakening its victims' government system.
- Convincing both the victim's population and its own the decay of the political system.
- Economic destabilisation.
- Influencing political decision-making to further promote the attacker's own agenda.

Through these goals, the attackers, both state and non-state actors, seek to destabilise the victim (another state, a specific community or group) while reinforcing their political vision and values amongst their own audiences.

A key component of hybrid threats: the digital technologies

Neither the objectives nor the means used to develop a hybrid threat are new. All of them have been used throughout history to weaken enemies without the need for conventional acts of warfare. The differential and key component of modern hybrid threats, which makes them more harmful than ever before, is the use of digital technologies. They have 'the unprecedented ability to use information as an element of warfare with much greater volume, velocity, breadth and depth and precision than previously possible, because global IT systems have made us more connected, more automated and allow for more precise messaging than ever before.' (Gibson, K. H., 2019).

In recent years numerous cases of hybrid threats where the technology component has become particularly important have been observed. One of the most serious and well-known was the cyberattacks in Estonia in 2007. Through distributed denial-of-service (DDoS), attacks targeted many institutions (the government, parliament, the police, etc.), businesses (banks, internet service providers) and critical infrastructure, causing an unprecedented national disruption and an extraordinary economic damage (Ottis, R., 2008).

More recently, probably the most mediatised case of a hybrid threat was the disinformation and meddling campaign -attributed to Russia (Mueller, R., 2019)- during the United States presidential elections in 2016 (US Senate, 2019). The attackers, GRU (Russian military intelligence agency) units, used cyberespionage techniques to hack Democratic Congressional Campaign Committee (DCCC) and Democratic National Committee (DNC) systems and steal sensitive information. GRU officers sent hundreds of phishing emails to Clinton Campaign employees and volunteers in order to steal accounts and credentials to gain access to the systems. Once the attackers accessed and stole the information, it was leaked to the public opinion through the website DCLeaks.com, the Guccifer 2.0 WordPress blog and Wikileaks at an opportune time, with the intention of weakening the Democratic Party candidate, Hillary Clinton, and preventing her election as US President (Mueller, R., 2019). In this case, the attackers also used fake accounts on social networks to magnify the impact of the disinformation campaign against Clinton's candidacy, based on the stolen information (Office of the Director of National Intelligence, 2017).

These few examples show the power of hybrid threats (and especially the impact of digital technologies in their informational components) to change others' beliefs, opinions, expectations, attitudes, preferences, emotions and willingness to act.

The scope of hybrid threats: from influence to hybrid warfare

As Hanna Smith, Director of Strategic Planning and Responses at the Hybrid CoE, has pointed out, the means of influencing, which is one of the main goals of hybrid threats, are more complex and multidimensional than just material means (Smith, H., 2017). Within the means of influencing, it is necessary to consider so-called ***soft power*** elements: education, cultural attractiveness, technology, science, diplomacy, good governance, etc. The influential capacity of different countries and actors in world politics may vary significantly and is not uniquely connected to so-called ***hard power***, aggressive and coercive measures in the military and economic spheres.

Both types of power, when properly combined, can be used to influence and take part in a hybrid threat. This was considered, for example, in the Strategic Defence Review of Georgia, which was approved in 2017. The Georgian government understood that the combined use of elements of *soft power* and economic pressure by a third party (Russia) against Georgia's national integrity represents one of the greatest challenges for its security environment (Ministry of Defence of Georgia, 2017).

The use of mechanisms of influence, based to a greater or lesser extent on soft power techniques, have led, for instance, to Russian businessmen linked to President Putin financing the think tank *Dialogue of Civilisations Research Institute (DOC)* in Berlin, which opened in 2016 (Treverton, G. et al., 2018). This think tank has been cited by several experts interviewed as a paradigmatic example of Russian attempts to influence Western countries through soft power measures.[4]

From everything mentioned, the combination of soft and hard power actions, usually in the form of hybrid threats, have become a key component of a new way of managing international relations and consolidating the influence of states. The problem is that this new scenario blurs the line between influence and interference in national affairs, and it is not always clear when the principle of non-intervention, and therefore international law, is violated.

The following table outlines a brief comparative analysis of means of influence. The comparison is based on two main characteristics: their novelty (columns) and their legitimacy[5] (rows). Hybrid threats usually encompass non-legitimate means, both traditional and non-traditional. However, legitimate means such as military exercises can also be used to reinforce the impact of hybrid threats.

Table 1: Comparison of means of influence considering their novelty and legitimacy

	Traditional	Non-traditional
Legitimate	- Security cooperation and foreign military sales - Economic sanctions - Military presence / engagements / exercises - Freedom of navigation exercises (maritime or aerospace domains	- Public diplomacy through non explicit support to IGO/NGO - Foreign internal defence - Misinformation / disinformation (non-criminal / freedom of expression)
Non-legitimate	- Political subversion by penetration or false-front organisations - Economic corruption - Propaganda / psychological operations - Sponsored criminal activity	- Disinformation (when it violates the rule of law) - Cyber intrusion / cyber corruption / disruption - Electoral interference

Source: (Hoffman, F. G., 2018)

[4] See Chapter 4.3.

[5] Legitimacy is understood as respect for international law and agreements

An actor (state or non-state) may increase the strength of a hybrid operation by intensifying one or more tools (military, political, economic, civil, information, cyberattacks, etc.) or by synchronising multiple tools in order to achieve a greater combined effect. The following figure shows the most important elements of so-called hybrid warfare, a concept used in the military context and analogous to that of a hybrid threat. Those elements in which the technological element is important or even decisive are highlighted in red.

Figure 1: Main components of hybrid warfare

Source: (Cubeiro, E., 2018)

In order to complement the analysis of the concept and scope of hybrid threats, the following section describes their most relevant components from a communication point of view, and the use of digital technologies.

2.1.1. Detailed analysis of the components of hybrid threats

As described above, hybrid threats encompass a wide range of means and tools to help the promoter achieve its goals. The following analysis will take into consideration the components suggested by Treverton, G et al. (2018).

Funding organisations and political parties for propaganda[6]

This component refers to the creation of organisations (think tanks, academic institutions) or political parties that promote and spread friendly visions amongst different groups (citizens, journalists, politicians, public servants, academics) according to the sponsor's interests. Indeed, this tool is one of the oldest means of political and social influence, the impact of which is now amplified by using digital services (social networks, online media outlets).

Russia can be considered one of the most active actors funding organisations in foreign countries. Allegedly Kremlin-funded think tanks are primarily focused on legitimising the Russian worldview by portraying a more favourable vision of its narrative and by defending its policies, even in operations of foreign influence (Hansen, F. et al., 2018). In addition to the aforementioned *Dialogue of Civilisations Research Institute*, the Kremlin think tank *Russian Institute for Strategic Studies (RISS)*, with offices across the Baltic states, has been accused of trying to hinder Montenegro's integration into NATO, meddling

[6] Propaganda can be defined as 'dissemination of information -facts, arguments, rumours, half-truths, or lies- to influence public opinion' (Lannes, B., 1999).

in Bulgaria's national elections (Treverton, G. et al., 2018), and defining a plan to influence the 2016 US presidential elections (Parker, N. et al., 2017).

China has also adopted this strategy to increase its foreign influence. For example, in 2015, Beijing promoted the creation of the think tank *Institute for China-American Studies (ICAS)* in Washington, the goal of which was to spread China's political vision amongst US politicians and economic leaders (Treverton, G. et al., 2018).

A similar approach has been used to economically support political parties with favourable views about the sponsor state. Some political parties from diverse Member States (France, Germany, Spain and Greece, amongst others) have been accused of receiving funds from foreign states in exchange for supporting their interests in Europe.[7]

Strategic leaks and cybertools

As the Hybrid CoE has pointed out, 'information and documents obtained via cyber or traditional espionage can be leaked to influence public opinion, perception, and discourse' (Treverton, G. et al., 2018, p. 50). Strategic leaks of information stolen through cyberespionage techniques can pursue diverse objectives, such as eroding of citizens' trust in democratic institutions (government agencies, political parties), damaging the reputation of public figures (politicians, public servants, journalists) or even blackmailing those public figures to act in favour of the leak promoter.

Cyber spies exploit computing system vulnerabilities to gaining unauthorised access and steal sensitive information. The information is usually leaked through specific websites such as Wikileaks at an opportune moment. One of the most dangerous tools used by cyber spies is the so-called *advance persistent threats* (APTs), which allow highly customised attacks to be carried out and can act for months, or even years, without being detected (Rivera, R. et al., 2017).

The most well-known cases (leaks of information stolen from the Democratic National Committee and the Clinton presidential campaign in 2016, and the leaks of e-mails related to the Emmanuel Macron campaign in 2017) were carried out in the context of presidential elections in two Western countries (USA and France) with the intention of influencing citizens' decisions and thus hampering the normal progression of the electoral process.

Apart from cyberespionage, ENISA (the European Union Agency for Cybersecurity) maintains a detailed taxonomy of cyber threats (ENISA, 2016), many of which can be used to develop a hybrid attack: (1) communication network outages; (2) interception of communications; (3) network traffic manipulation; (4) critical infrastructure sabotage; (5) identity theft; (6) distributed denial-of-service (DDoS); (7) malware; (8) manipulation of information.

Social media and domestic media outlets

Propaganda campaigns are often aimed at both foreign and domestic audiences. These campaigns use both traditional media outlets (TV and radio channels) and digital means (social networks), adapting the messages to each audience. When media outlets, whether traditional or digital, are sponsored by specific states, they tend to spread information from the perspective of those state sponsors. That is the case of two well-known media outlets, Sputnik and RT, which have delegations in many Western countries and content in several languages, the main objective of which is to inform Western citizens about current events from the Kremlin's perspective, favouring Russian interests.

Social media platforms are helping perpetrators develop new forms of influence. They allow the information offered by foreign official media to be altered, increasing the diffusion of information provided by local media, as well as generating new information through state-sponsored accounts. This was the case of Russian influence in the US presidential elections. Disinformation began in foreign

[7] (Oliveira, I., 2016); (Sciorilli, S., 2019); (Marcos, J., 2016); (Foster, P. & Holehouse, M., 2016).

media outlets such as RT or Sputnik. Then, it was amplified on a mass scale through bots and trolls on social networks (mainly Twitter and Facebook), which finally facilitated its spread through traditional media.

While the use of traditional media outlets for propaganda campaigns are aimed at broad audiences, with almost no segmentation capacity, social media platforms represent a great opportunity to spread personalised messages to very specific audiences. The vast amount of information that social media platforms have about their users can be exploited to profile them and define microtargeting campaigns according to those profiles, improving the effectiveness of propaganda.

Paramilitary organisations

It is also necessary to point out the role played by paramilitary organisations in hybrid conflicts. They act as local proxies following orders from foreign governments, without revealing their origin. The use of diverse paramilitary organisations has been witnessed in recent conflicts, such as the so-called *Night Wolves*, a Russian ultranationalist motorcycle club with different branches in Eastern European countries (Peter, L., 2018). One of its most relevant interventions took place during the Crimean crisis, intimidating the civilian population that opposed the referendum to decide on the annexation to Russia. Other examples, also related to the illegal annexation of Crimea by Russia and further attacks by Russian-backed forces in the Donbass region (eastern Ukraine), are the *Russian Orthodox Army*, the *Vostok Battalion,* the *neo-Cossacks* (Darczewska, J., 2017) and the so-called *little green men*. This last armed group, equipped with modern weapons, deployed masked soldiers in green military uniforms without any type of identification or badge. Although they were part of the Russian armed forces, as the Russian President Vladimir Putin finally admitted (Schreck, C., 2019), they operated in a covert manner in order to hide their connection with the Russian government. This way Russia could avoid formal warfare with Ukraine and military responses from intergovernmental organisations such as NATO.[8]

Religious influence

Mechanisms of influence can also be deployed by making use of religious matters. For example, the Russian government has been trying to use religious influence to support the Kremlin's interests in European countries. The diverse local churches within the Orthodox Church can be used not only to tighten the bonds between communities, which may be positive, but also for influencing minorities or exacerbating nationalist sentiments. The other way around, the Russian Orthodox Church has influenced the ideological motivations related to internal security among Russian politicians and military leaders, trying to gradually paint the national defence of Russia as a spiritual and holy mission (Adamsky, D., 2019).

Religion is also used by other state and non-state actors to influence religious believers in foreign countries. It is well known that the spread of religious propaganda through social networks by terrorist groups like ISIS or Al Qaeda is used to justify their terrorist attacks and inflame their supporters around the world. Countries such as Saudi Arabia or Iran also use religion to expand their influence beyond their borders. They are the most powerful countries in the Middle East and the main representatives of the two major branches of Islam: Sunni Islam (Saudi Arabia) and Shia Islam (Iran). Religious matters are often used to influence both neighbouring countries and the Muslim population in other regions. For instance, Saudi Arabia is one of the greatest financers of Salafist mosques and Islamic centres in EU countries (AOAV, 2017), from where one of the most conservative ideologies within Sunni Islam, Salafism, is spread.[9]

[8] Although Ukraine was not a NATO member country at the time of the Crimea's invasion by Russia, they cooperated closely.

[9] For more details, see Chapter 4.1.

Economic pressure

Means of influence based on economic aspects are also very effective as elements of pressure, and can have different forms: foreign aid, use of borrowed resources, foreign influence in strategic economic sectors (energy, tourism, agriculture, etc.) (Treverton, G. et al., 2018). These have been common practices in most recent conflicts. China, given its economic power, is one of the international actors that most uses economic pressure to threaten its competitors and broaden its influence.

Concerns about migration

Migration can be considered another relevant component of hybrid threats when it is used by a state actor as a mechanism to pressure or influence other countries or international organisations. Promoters take advantage of Europeans' concern regarding this topic, as reflected in recent official surveys (Eurobarometer, 2019, p. 15). At present, some countries use migration as a political weapon to coerce other states to act in a certain way. One of the most notorious cases in the EU refers to the Turkish use of migrants as a pressure element at the Greek border. Diverse indicators, mainly data from the UN Refugee Agency, showed an increase in migratory flows through the Evros river, the natural border between Greece and Turkey, which was the result of tensions in Greek-Turkish relations. The Greek authorities confirmed the deliberate impassibility of the Turkish border guards, allowing large groups of refugees to cross their border with Greece to pressure Athens and Brussels on visa liberalisation for Turkish citizens (Euroactiv, 2018).

Like other components of hybrid threats, this phenomenon can hardly be managed autonomously by each country. In the EU, a comprehensive approach that takes into account European interests as a whole is still lacking, as Member States act according to their needs, perceptions and circumstances, supporting the initiatives that best match their interests (Fine, S., 2019). An example of this lack of common vision about migration among EU countries can be found along the shore of the Mediterranean. While some Mediterranean EU countries denied NGO vessels devoted to rescuing migrants off the coasts of Maghreb countries (mainly Libya) access to their ports,[10] other EU countries willing to host those migrants found it very difficult to do so (Sanders, L., 2019).

Russia, the most active promoter of hybrid threats against Western countries

Russia has been identified by most of the experts interviewed as the major state actor in using hybrid threats against Western countries. Because of its importance in the international context, the following table, based on (Davis, J. R., 2015), shows a compendium of the most significant hybrid actions that the Russian government has deployed in recent years (especially during the illegal Crimean annexation), in support of its claims.

Table 2: Components of hybrid threats used by Russia

Level	Action
Tactical level	- Combination of irregular and tactical forces with advanced conventional weapons and elite regular military special operations forces (Spetsnaz) pursuing a common objective. - Use of combatants linked to irregular units and local pro-Russian criminal gangs. - Use of cyber-attacks against critical communication infrastructure to interrupt the flow of information and allow the Russians to obtain information about enemy intentions and actions.

[10] The most notorious example was the conflict between Italy and the NGO Sea Watch in June 2019, which concluded with the arrest of the Captain Carola Rackete after 60 migrants rescued off the Libyan coasts disembarked in Lampedusa, defying the Italian banning on NGO vessels bringing migrants to the Italian coasts (Holroyd, M., 2019).

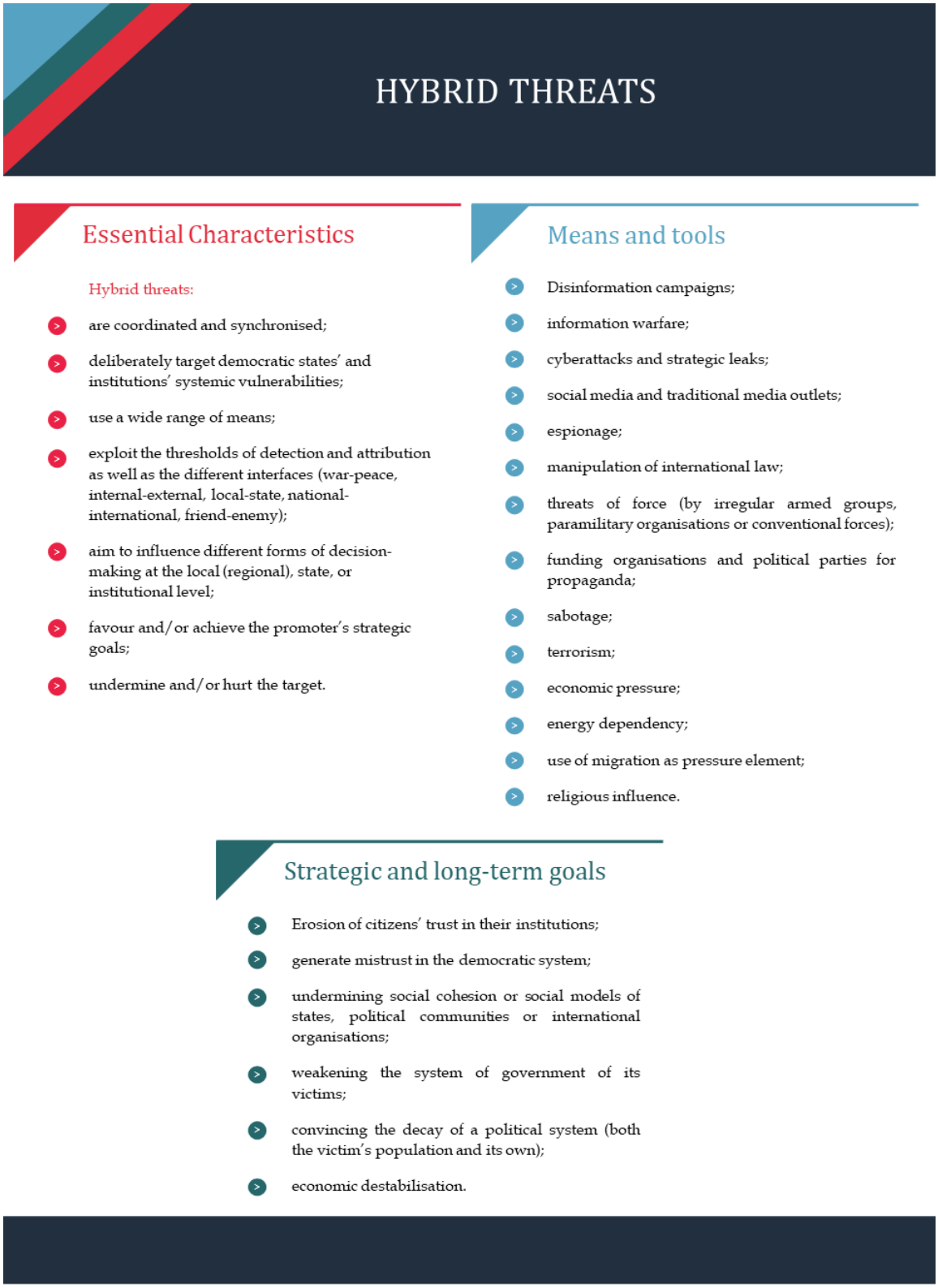
Operational level	- Linking tactical level actions with information operations to achieve an operational level of deception. - Deployment of conventional military capabilities along the borders with the target countries, conducting demonstrations and training exercises that divert attention from other operations. - Covert movements of arms and paramilitary elements under the cover of humanitarian aid to the ongoing crisis. - Performing psychological and informational operations to help achieve the operational deception. These operations incite violence to force people to act when necessary. Conversely, they can also intimidate and coerce people into not acting.
Strategic level	- Synchronisation of all IOPs (Instruments of Power) towards a common goal. - Exploiting information from IOPs to build competing strategic narratives that affect multiple audiences: o External and international audiences: Russia employs a strategic narrative that gains the support of international organisations seeking peaceful resolution of conflicts. o Domestic audiences: Russia promotes a strategic narrative aimed at maintaining internal support by combining the exaltation of nationalism and denouncing the oppression of its own people in foreign countries. - Use of diplomatic 'ceasefire' as a tactical pause in ongoing operations, to consolidate, reorganise and relocate forces to achieve a position of relative advantage for future missions, allowing Russia to resume hostilities again at the time and place it chooses. - Use of economic IOPs to threaten and coerce other nations into action or inaction. Economic sanctions, destabilisation of energy prices and physical access to energy resources, and the actions of transnational criminal organisations can deter a country from acting. - Exhibition (more or less veiled) of the enormous destructive capacities of cyber-attacks against financial and/or energy infrastructure. The Russian government has been able to combine various forms of paramilitary action with economic, intelligence and diplomatic IOPs, under an integrated approach, which has allowed it to keep the conflict below the minimum threshold required to invoke the collective defence guarantee of Article 5 of the NATO Treaty.

Source: (Davis, J. R., 2015)

Summary of hybrid threats' components

The following image summarises the characteristics of hybrid threats, the means and tools used to carry out such threats, and the strategic and long-term goals they pursue.

Figure 2: Summary of the features of hybrid threats



Source: own elaboration based on desk research and interviews

2.1.2. The special role of disinformation campaigns

As the Joint Research Centre has pointed out, the term 'fake news' is a newcomer to the news media vocabulary, especially since the US presidential elections in November 2016, when its use became widespread (Martens, B. et al., 2018). However, the European Commission, following the suggestions of the High Level Expert Group on fake news and online disinformation, has opted to use the term *disinformation* for two main reasons (High Level Group on fake news and online disinformation- European Commission, 2018, p. 10):

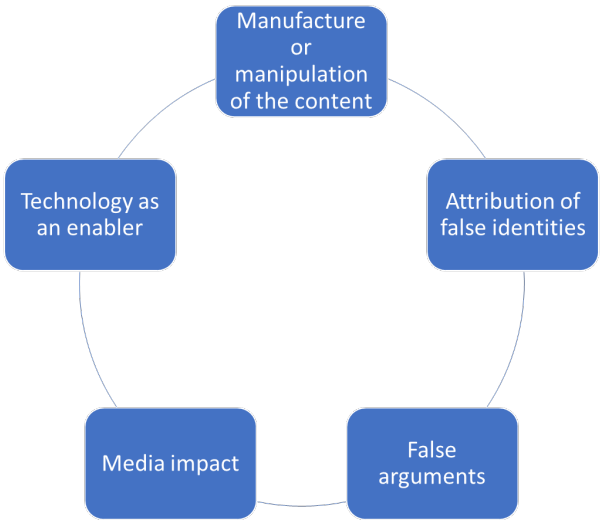
1. The term 'fake news' does not adequately reflect the complexity of disinformation. Disinformation implies not only the use of fake content but also fabricated information blended with real facts, and goes beyond news creation.
2. The term 'fake news' has been appropriated by some politicians and their supporters, who use it to dismiss any unfavourable information related to them and to discredit critical news media.

Disinformation can:

- 'threaten democratic political and policy-making processes;
- put the protection of EU citizens' health, security and their environment at risk;
- erode trust in institutions and in digital and traditional media;
- harm democracy by hampering the ability of citizens to take informed decisions;
- polarise debates;
- deepen tensions in society;
- undermine electoral systems' (European Commission, 2019d).

Disinformation is created by distorting the reality with the aim of generating confusion amongst citizens and exacerbating political polarisation and division. Foreign governments or domestic populist movements can leverage the effects of disinformation to weaken the social and political landscape of the countries attacked. The following figure shows the five essential elements of disinformation which, when properly combined by the attacker, represent its greatest danger.

Figure 3: Components of disinformation campaigns



Source: own elaboration

The first phase of a disinformation campaign is the creation of manipulated content, which usually addresses a real fact from a distorted perspective. After the fake content is fabricated, disinformation promoters try to attribute it to reputable sources. This has two main goals: to increase the credibility of the false information in order to amplify its impact, and undermine the reputation of the source when the disinformation is discovered. The fake content is complemented and backed through false arguments, and relies on media outlets and digital platforms to reach broad audiences and meet its goals: misleading the public opinion to undermine social and political cohesion and weaken democratic institutions.

Disinformation campaigns take advantage of the numerous options for spreading information that have been opened up by digital platforms. They allow fake content to be developed and disseminated, thanks to the use of bot accounts, which have a credible, professional appearance and a low cost, and without requiring high journalist skills. They also allow direct connection with the targeted audiences, bypassing traditional gatekeepers (news editorial committees) and avoiding fact-checking (European Commission, 2018a).

Disinformation campaigns promoters also seek another objective: delegitimising one of the fundamental actors in democracies, the journalism sector. They try to undermine citizens' trust in media outlets, companies and specific journalists in order to enhance the credibility of false information: if no media outlet or journalist is reliable, false information becomes as credible as any other information, increasing its impact (Hybrid CoE, 2019). According to the Special Eurobarometer 503 (European Commission, 2020d), 62 % of European citizens consider media outlets the principal agents to combat disinformation, surpassing public authorities (53 %), social media platforms (48 %), the citizens themselves (28 %) and educational institutions (22 %). Given the key role that citizens give to media outlets in the fight against disinformation, it is not surprising that one of the first goals of any disinformation campaign is to undermine their reputation.

Another major issue when dealing with disinformation spread through digital means is the so far unresolved dilemma of social media platforms' responsibility on the veracity of content. The legal status of social media platforms regarding key aspects such as transparency or accountability remains undefined, in contrast with the relevant regulation to which the media sector is subject (Hybrid CoE, 2019). This issue is increasingly relevant, as online social networks and other online channels are extensively used by citizens of all ages to access news: 88 % of people under 25, 85 % of people aged between 25-50 and 70 % of people over 50 use social media weekly to stay informed (European Commission, 2018a). Despite high levels of use, these channels (social networks, online news aggregators and online blogs) are the least trusted by citizens (European Commission, 2018a).

The phenomenon of disinformation is not easy to measure. For instance, the EUvsDisinfo Database,[11] part of the flagship project of the East StratCom Task Force, includes over 6 500 examples of pro-Kremlin disinformation[12] collected since the launch of the project (May 2015). However, the real impact of each piece of disinformation is unknown.

The Oxford Internet Institute tried to quantify and describe organised online disinformation and propaganda campaigns around the world (Bradshaw, S. & Howard, P., 2019). According to this source, the number of countries where such campaigns have taken place increased from 28 in 2017 to 70 in 2019. The campaigns in each country were promoted by one or various actors: government agencies, politicians and political parties, private contractors, civil society organisations, or citizens and influencers. Regarding the techniques and tools, 87 % of countries used human accounts to spread propaganda and disinformation on social media platforms, 80 % used bot accounts (automated accounts designed to mimic human behaviour online), 11 % used cyborg accounts (which mix automation with human treatment of the content) and 7 % used hacked or stolen accounts. The

[11] https://euvsdisinfo.eu/disinformation-cases/

[12] Data consulted in January 2020.

objectives ranged from using propaganda to attack political opposition (89 % of countries), spreading pro-government or pro-party ideas (71 %), suppressing participation through personal attacks (63 %), driving division and polarisation (34 %), and distracting conversations and criticism away from important issues (20 %).

The most widely used communication strategy was the creation of disinformation and media manipulation (75 % of countries). 73 % of countries contributed to disinformation campaigns by amplifying their impact (for instance, using specific hashtags on a mass scale), 68 % used state-sponsored trolls to attack political opponents, 27 % developed data-driven strategies to target specific communities with disinformation and 16 % reported content or accounts on a mass scale (usually critics of the government or political party) in order to get them taken down by social media platforms' automated systems (Bradshaw, S. & Howard, P., 2019).

While the above figures refer to campaigns developed internally in each country, two of the main social networks, Facebook and Twitter, have pointed to seven countries as the most active in foreign influence operations through social media services: China, India, Iran, Pakistan, Russia, Saudi Arabia and Venezuela (Bradshaw, S. & Howard, P., 2019). The following table summarises, based on the information collected by the Oxford Internet Institute, the capacities, tools and strategies developed by these countries to create disinformation campaigns.

Table 3: Capacities for developing disinformation campaigns in selected countries

	CYBER TROOP CAPACITY	TYPES OF FALSE ACCOUNTS	MESSAGING STRATEGIES	COMMUNICATION STRATEGIES
China	**HIGH CAPACITY** Team size: estimates of 300 000-2 000 000 people working in local and regional offices	Bots Human	Spreading pro-government or pro-party propaganda; Attacking the opposition or mounting smear campaigns; Distracting or diverting conversations or criticism away from important issues; Suppressing participation through personal attacks or harassment.	Creation of disinformation or manipulated media; Mass-reporting of content or accounts; Data-driven strategies; Trolling, doxing or harassment; Amplifying content and media online.
India	**MEDIUM CAPACITY** Multiple teams ranging in size from 50-300 people. Multiple contracts and advertising expenditures valued at over 1.4M USD	Bots Human	Spreading pro-government or pro-party propaganda; Attacking the opposition or mounting smear campaigns; Driving division and polarisation;	Creation of disinformation or manipulated media; Data-driven strategies; Trolling, doxing or harassment; Amplifying content and media online.
Iran	**HIGH CAPACITY** 6 000 USD spent on FB advertisements	Bots Human Stolen or hacked accounts	Spreading pro-government or pro-party propaganda; Attacking the opposition or mounting smear campaigns; Suppressing participation through personal attacks or harassment.	Creation of disinformation or manipulated media; Mass-reporting of content or accounts; Data-driven strategies; Trolling, doxing or harassment; Amplifying content and media online.
Pakistan	**MEDIUM CAPACITY**	Bots Human	Spreading pro-government or pro-party propaganda;	Creation of disinformation or manipulated media;

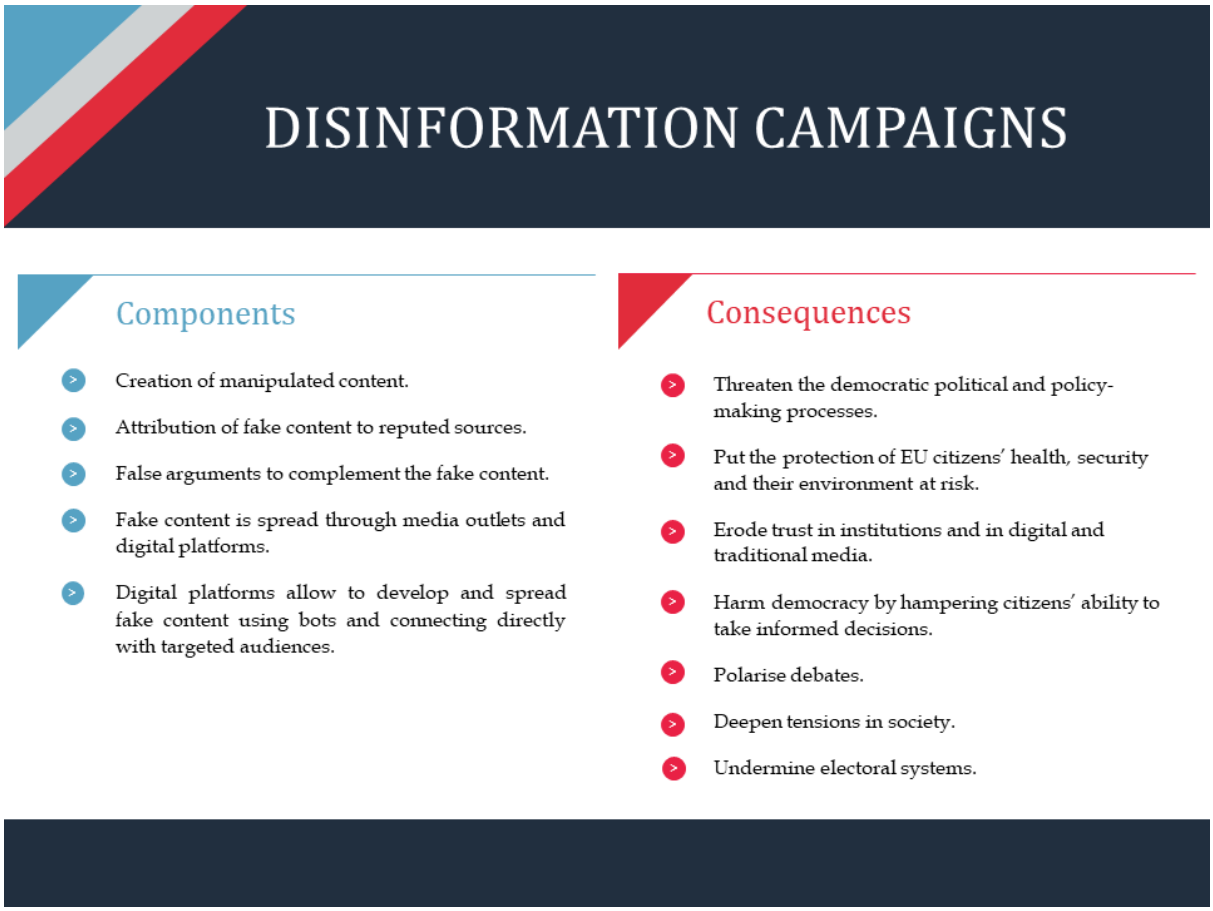
	(No specific data)		Attacking the opposition or mounting smear campaigns; Suppressing participation through personal attacks or harassment.	Data-driven strategies; Amplifying content and media online.
Russia	**HIGH CAPACITY** (No specific data)	Bots Human Cyborg accounts Stolen or hacked accounts	Spreading pro-government or pro-party propaganda; Attacking the opposition or mounting smear campaigns; Distracting or diverting conversations or criticism away from important issues; Driving division and polarisation; Suppressing participation through personal attacks or harassment.	Creation of disinformation or manipulated media; Mass-reporting of content or accounts; Data-driven strategies; Trolling, doxing or harassment; Amplifying content and media online.
Saudi Arabia	**HIGH CAPACITY** Estimated costs of 150 GBP for Twitter hashtag trends	Bots Human Cyborg accounts	Spreading pro-government or pro-party propaganda; Attacking the opposition or mounting smear campaigns; Driving division and polarisation; Suppressing participation through personal attacks or harassment.	Creation of disinformation or manipulated media; Trolling, doxing or harassment; Amplifying content and media online.
Venezuela	**HIGH CAPACITY** Team size estimates of multiple brigades of 500 people. Evidence of formal training	Bots Human	Spreading pro-government or pro-party propaganda; Attacking the opposition or mounting smear campaigns; Distracting or diverting conversations or criticism away from important issues; Suppressing participation through personal attacks or harassment.	Creation of disinformation or manipulated media; Trolling, doxing or harassment; Amplifying content and media online.

Source: (Bradshaw, S. & Howard, P., 2019)

Disinformation campaigns are not only used in the civil sphere. The disinformation element is also considered a major military component. Valery Gerasimov, the Chief of Staff of the Russian Armed Forces since 2012, who is considered the father of using disinformation as an essential part of modern military doctrine (McKew, M., 2017), pointed out the challenges of new forms of warfare in his essay '*The value of science is in the foresight*'. He argued that 'the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy' (Gerasimov, V., 2013, p. 27).

The following figure summarises the main features of disinformation campaigns.

Figure 4: Main features of disinformation campaigns



Source: own elaboration based on desk research and interviews

2.2. Taxonomy and key characteristics of response actions

Combating hybrid threats, especially when they include disinformation components, is a difficult task and a great challenge for liberal democracies, since the measures adopted, in addition to being able to neutralise the impacts of the threats, must respect the exercise of fundamental rights, such as the rights to freedom of expression and freedom of information. These are restrictions that do not apply in authoritarian and undemocratic states.

An effective way to classify the necessary countermeasures is by **looking at when** they should be taken. Thus, they can be categorised as:

1. **Preventive measures**: aimed at taking all necessary precautions to ensure that hybrid threats do not materialise or that, if they do, damage is eliminated or limited. Deterrence tools are considered a kind of preventive measure.
2. **Detection measures**: aimed at discovering when one is a victim of a hybrid threat.
3. **Response measures**: aimed at responding effectively to a hybrid threat when it has already materialised, including measures to restore affected systems to their original condition, and even offensive actions against the attackers (diplomatic, economic, military, informative, etc.).

The following table shows a high-level taxonomy of measures that can be adopted at different levels (political, diplomatic, informative, economic, intelligence and legal) to counteract hybrid threats according to the described temporal model.

Table 4: Taxonomy of measures to counter hybrid threats

	PREVENTIVE measures	DETECTION measures	RESPONSE measures
Political or diplomatic actions	• International agreements on the limits of influence, what interference is and applicable sanctions. • Identification of potentially harmful stakeholders and clarifying their links with the offending countries. • Collaborative measures with international organisations for the defence of protected interests, such as NATO. • Risk assessments to identify vulnerabilities (social, economic, technical, etc.).	• Fast and efficient supranational communication procedures for coordinated action.	• International sanctions for those countries that have caused a hybrid threat. • Personal sanctions for 'creators or inspirers' of hybrid threats (leaders, political or commercial representatives, etc.).
Informative actions	• Awareness-raising campaigns on the danger of news spilledin unreliable media, particularly in times of special relevance (such as election periods). • Increase media capacity to detect and publicise potential risks to the reputation of a group, organisation or even the State itself. • Promote education in detecting and preventing hybrid threats from an early age. • Develop training initiatives amongst vulnerable groups: elderly people, people with low digital literacy skills.	• Clarify the role of social media platforms in the detection of disinformation campaigns. • Promote the role of fact-checkers and create communication and collaboration channels with the authorities (government, judiciary, law enforcement agencies). • Foster civil engagement to detect disinformation and exposure the promoters. • Increase monitoring of digital channels to quickly discover disinformation campaigns	• Publicise and disseminate the attribution of a threat. • Inform citizens of behavioural patterns for damage control. • Warn the attackers of the consequences of developing new hybrid threats.
Economic of financial actions	• Increase economic, energy and technological independence from risk countries or providers. • Increase investments in R&D related to technologies that allow detecting and preventing	• Increase economic resources allocated to detection of disinformation.	• Increase economic resources allocated to attribution of threats. • Economic sanctions for

	hybrid threats (AI, human language technologies, cybersecurity, 5G, blockchain). • Increase budget for raising awareness.		offending countries. • Economic sanctions for stakeholders (organisations, groups or individuals, domestic or foreign) that have benefited from the effects of a hybrid threat.
Intelligence actions	• Expand resources and expert training, including joint exercises between Member States to learn how to face hybrid threats in a coordinated way. • Identification of domestic stakeholders that could collaborate in the spreading of the hybrid threat.	• Secure and rapid communication channels with stakeholders to provide information on detected threats. • Development of detection tools against hybrid threats and fake content. • Increase public-private information sharing.	• Foster international information sharing. • Enhanced coordination response mechanisms between Member States and foreign partners.
Legal actions	• Clarification of the legal responsibilities of different stakeholders. • Ensure that legislation is appropriate for digital environments and channels. • Harmonisation of the legal framework in the EU.	• Ensure that legislation is appropriate for digital environments and channels.	• Ensure that legislation is appropriate for digital environments and channels. • Legislative simplification for rapid response to threats.
Military actions	• Guarantee appropriate military expertise on the whole scope of hybrid threats. • Improve coordination between different corps and with the civil authorities.	• Rapid and cohesive response plans and strategies.	• Proportional military actions.

Source: own elaboration from desk research and interviews

3. Strategic communications as response to hybrid threats

The response to hybrid threats demands coordinated action in different domains. Response actions alone are not enough to effectively counter the impacts of hybrid threats. If they are not adequately communicated to the specific audiences, in a timely manner and with precise messages, through the appropriate channels and formats, they will not meet their goals and the hybrid threat will be successful. In a society overloaded with information and contradictory messages, strategic communications are key to developing a retaining wall for countering the constant flow of disinformation, misinformation, cyberespionage, leaks of stolen information, digital harassment, manipulation and other forms of information used by promoters of hybrid threats. This chapter is focused on analysing the concept of *strategic communications*, in other words, how strategic communications can contribute to countering hybrid threats, what their main elements are and what related initiatives have already been implemented. And all this without losing sight of the role played by digital technologies as a support for any communication strategy.

3.1. Concept and scope of strategic communications

When analysing the concepts of hybrid threats and disinformation, there seem to be many definitions of the term 'strategic communications'. In a report produced for the European Parliament by the European Union Institute for Security Studies, strategic communications are defined as 'communications activities with an agenda or a plan' (European Union Institute for Security Studies, 2016, p. 4). Several sources (such as (Cornish, P. et al., 2011) and (Tasiu, A., 2018)) cite the following definition: 'Systematic series of sustained and coherent activities, 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' (Tatham, S., 2008, p. 3). NATO has also produced its own definition: 'The coordinated and appropriate use of NATO communications activities and capabilities -Public Diplomacy, Public Affairs, Military Public Affairs, Information Operations and Psychological Operations, as appropriate- in support of Alliance policies, operations and activities, and in order to advance NATO's aims' (NATO, 2009b). From these definitions, and the ideas collected from interviews with experts, the essential characteristics of strategic communications can be summarised as follows:

- They are executed according to a predetermined and systematic plan, not only as a reaction to current events;
- They involve actions at strategic, operational and tactical levels;
- They are developed in a competitive, and even conflictive, environment, where audiences are subject to a constant buzz that can hamper meeting their goals;
- They demand a high level of coordination and synchronisation between stakeholders;
- They require specific definition of the targeted audiences;
- They require selection of the most adequate communication channels;
- They aim to inform, influence or promote behavioural changes in target audiences;
- They must be aligned with the overall goals of the promoter country or organisation;
- They must focus on both the short and long terms.

Strategic communications are not only about words or messages. Actions can also be a powerful communication tool and should be taken into account when defining a communication strategy (Silvela, E., 2017).

Obviously, not all kinds of communication can be dubbed as *strategic*. Emily Goldman, current Director of the US Cyber Command/National Security Agency Combined Action Group, has detailed the differences between strategic and non-strategic communications:

Table 5: Strategic vs. non-strategic communications

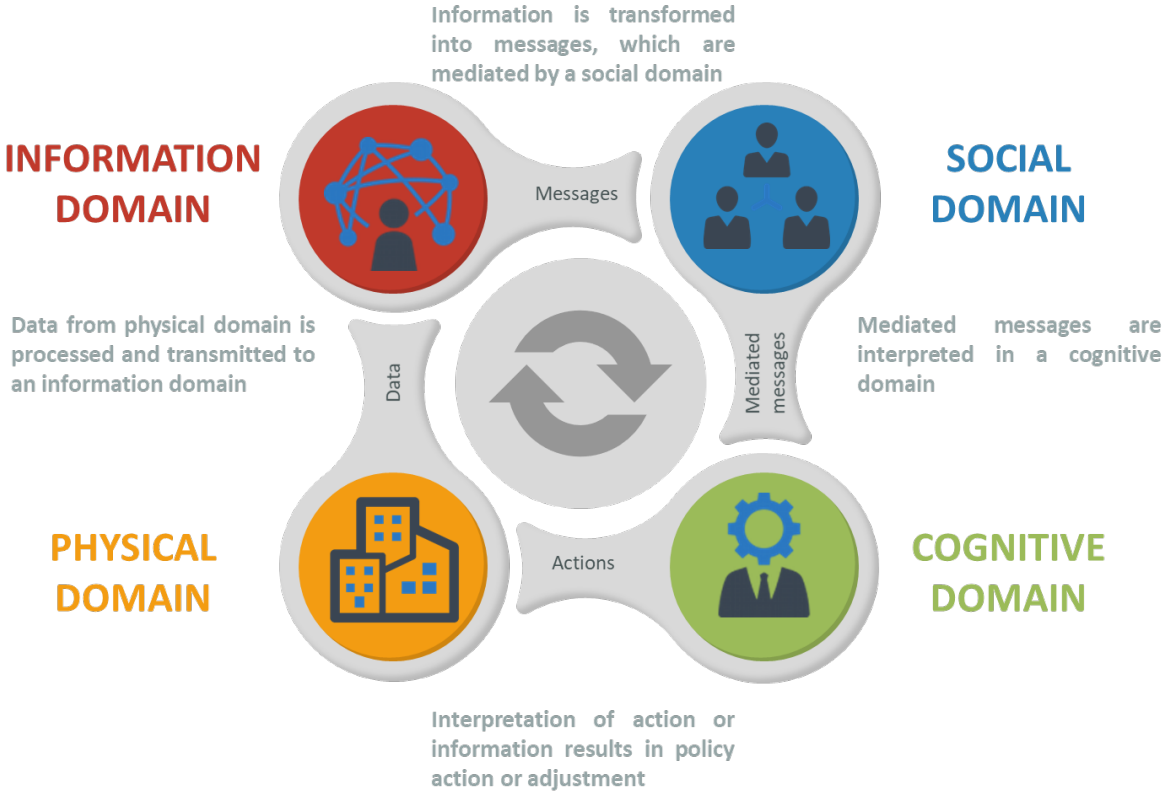
	Strategic	Non-strategic
Scope	Multiple and diverse audiences	Bounded and general audience
Time	Continuous	Discrete
Objective	Advance policy goals	Deliver a specific message to a specific audience at a specific time
Measure of effectiveness	Degree of policy advancement	Meeting deadlines
Communication means	Receiver-centric	Sender-centric

Source: (Goldman, E., 2007)

Strategic communications target multiple audiences and are planned for long periods of time, with continuous activities. Their main objective is to advance the policy goals for which they were defined, and their effectiveness can be measured by the degree of progress towards those goals. Finally, they adapt communication means (contents, channels) to the characteristics of the receiver. On the contrary, non-strategic communications adopt a more generalist approach and encompass discrete actions at certain moments without considering the specificities/characteristics of the audience.

It is important to note, mainly to understand the impact of digital technologies in the communication process, that strategic communications are developed in four domains (Goldman, E., 2007), as it can be seen in the following image.

Figure 5: Strategic communications domains



Source: (Goldman, E., 2007)[13]

The events take place in the physical domain. The information domain processes data collected from those events and creates the messages, which are mediated by the social domain through cultural, political, social and historical visions. The mediated messages are interpreted by individuals in the cognitive domain, becoming feelings (hope, concern, fear, etc.), changes in attitudes or behaviours, or actions, whose interpretation derives in policy adjustments over the physical domain. A comprehensive and successful strategic communication should work on and control the flow of information in the four domains (Goldman, E., 2007).

Principles of strategic communications

According to the doctrine proposed by the US Department of Defence, strategic communications should be developed under nine principles (US Department of Defence, 2008):

- **Leadership-driven**. Organisation leaders must assume the responsibility of driving strategic communications. Success heavily depends on a clear leadership, which should materialise in the alignment of the organisation's overall goals with strategic communication objectives. Leadership should also provide proper resources for strategic communications.
- **Credible**. Credibility, accuracy, truthfulness, trustworthiness, consistency and respect are essential premises for effective strategic communication.
- **Understanding**. Strategic communications require making an effort to know and understand cultures, visions, identities, history, attitudes, behaviours and social values of the targeted audiences. This understanding is key to adapting messages and actions in order to be well received by the targeted groups. Close collaboration with targeted communities (civil

[13] Template designed by Showeet.com

associations, academic institutions, economic agents, etc.) is necessary to better understand audiences' beliefs and values.

- **Dialogue**. The exchange of ideas and mutual comprehension between all parties involved must be considered when building strategic communications. Promoters should listen and respect audiences' opinions to create an adequate response.
- **Pervasive**. Every action, word and image sends a message. Communication must be permanent, and any organisation member can act as a messenger. Promoters of strategic communications should be aware of the unintended consequences of the messages transmitted and be capable of tackling them.
- **Unity of effort**. The definition and execution of strategic communications is a collaborative process where coordination and synchronisation are indispensable requirements, both from a vertical (from tactical to strategic level within a department) and transversal perspective (among different departments).
- **Results-based**. Strategic communications must have a clear objective and must focus on achieving the desired results.
- **Responsive**. Although strategic communications must be focused on the long term, they should be flexible enough to evolve rapidly in the short term when conditions change, or crises appear.
- **Continuous**. Strategic communication is a continuous process of research, data collection, analysis, planning, implementation, assessment and adaptation.

Some of these principles would be almost impossible to implement without the incorporation of digital technologies. They contribute to synchronising actions and messages, to better understanding the audiences and continuously adapting the information to their particularities, and to creating the adequate communication channels to enhance the effectiveness of the strategy.

Challenges of strategic communications

Large institutions, such as the EU or Member State governments, have many internal and foreign interests, which usually involve multiple audiences and a great range of topics. Given the vast amount of issues that these institutions must manage, they tend to adopt a reactive approach when implementing strategic communications (European Parliament, 2016d). However, this also entails a great risk of losing control of the communication process. Therefore, a new mindset is necessary amongst leaders in order to drive strategic communications in a proactive way.

One of our main values is democracy. And democracy implies openness, transparency and debate, attributes that promotors of hybrid threats can use to exploit the vulnerabilities of the democratic system. However, strategic communications developed by democratic institutions (the EU, Member States) cannot rely on measures, tools or techniques that betray democratic values. It is, therefore, necessary to assume that democracies are facing an asymmetric fight between those who have no objection to using illegitimate or illegal methods to achieve their goals, and those who must respect democratic rules.

The last relevant challenge is bureaucracy. It hampers three of the above principles: leadership, unity of effort and responsiveness. Managing strategic communications in large bureaucratic institutions requires great leadership skills. It also demands a great capacity for rapid and coordinated reaction, for which slow bureaucratic processes are not always ready.

Strategic communications at a glance

The following image summarises the main features of strategic communications.

Figure 6: Main features of strategic communications

Source: own elaboration based on desk research and interviews

After analysing the concept of strategic communications, Chapter 3.2 examines its constituent elements, with special emphasis on the role of digital technologies.

3.2. Elements of strategic communications

The fundamental elements of strategic communications are the *desired result, the audience, the message, the methods to communicate and the impact assessment* (Baños, P., 2011).

The precise definition of the **pursued result** is the cornerstone to building an effective strategic communication. Not only must the desired results be appropriately identified, they must also be included in the strategy plans from the very beginning. Thus, all agents involved can interiorise them and focus all their activity on achieving them.

Audiences are probably the element that most influences the definition of strategic communications. They can be defined in terms of geography (foreign or domestic audiences), type of relationship (allies, adversaries) or type of groups (whole society, governments, supporters of adversaries, insurgent groups, terrorist groups). Regarding domestic audiences, one of the main goals of strategic communications is to improve society's resilience hybrid threats, informing the citizens about the risks and how to deal with them. In the international sphere, strategic communications are aimed at gaining the support of allied countries on specific actions (diplomatic, military, economic) to face hybrid threats. Strategic communications must also target the promoter of hybrid threats, whether domestic or foreign. Depending on the timing of the threat, they can range from deterrence campaigns (threatening the attacker with economic sanctions, showing the military power, etc.) to more aggressive measures. After being processed using big data tools, the vast amount of information about individuals and communities collected from communication networks allows microtargeting techniques to be used to segment audiences with an enormous precision. This contributes to increasing the efficiency of messages and actions included in the communication strategy.

Messages can adopt multiple forms. From written information to videos, or even on-site operations, they should be designed to provide a strategic narrative. This can be defined as 'a story designed to provide an emotive justification for a policy goal, and in many cases how that goal is to be realised and the moral authority for doing so' (UK Ministry of Defence, 2019, p. 6). A strategic narrative should encompass the following content:

- the current situation, describing what you want to modify or preserve;
- the future state that you intend to achieve;
- the pathway to get there;
- and the justification, the reason why you seek to change the situation.

Within strategic communications, the **methods used to communicate** are as important as the narratives. Methods refer to both communication models and technical means. Regarding communication models, we can differentiate between monologue (unidirectional) and dialogue (bidirectional). Monologue has been one of the most used communication models, although it can be considered less effective, especially when dealing with foreign audiences (Goldman, E., 2007). Effectiveness of monologue is limited to hierarchised environments (for instance, an army). On the contrary, strategic communications regarding multicultural scenarios require dialogue techniques.

Any communication strategy should use all technical means at its disposal. However, they should be adequately adapted to the preferences and needs of the targeted audiences. Both traditional means such as live TV and radio, newspapers, magazines, etc., and online services (social networks, blogs, podcasts, instant messaging apps, video platforms, etc.) can be useful to communicate the messages. Chapter 3.2.1 analyses in detail the impact of the most recent technological developments (artificial intelligence, IoT, 5G, blockchain) in the means and tools available for strategic communications.

It is important to note that strategic communications not only entail the use of technical means for remote communications. They can also require person-to-person interactions, reconnaissance trips, personal meetings and any other kind of physical exchange of information.

The finally important element of any strategic communication is the **impact assessment**. It is important to define strategies and metrics that allow evaluation of whether the messages transmitted have achieved their objectives:

- Have they reached the targeted audiences?
- Have they been understood by the targeted audiences, who are behaving according to the expected results?
- Have they produced unintended consequences because they have reached unexpected audiences?

Depending on the level of fulfilment of the objectives, the communication strategy can be maintained or redefined.

Digital technologies are a constituent part of the elements of strategic communications. The following chapter analyses how they are being used and the role that the latest technological developments are playing.

3.2.1. Impact of digital technologies on strategic communications

Digital technologies impact strategic communications in several ways. From the communication infrastructure itself to the most advanced communications services, digital technologies open up great opportunities to spread messages amongst broad audiences in a rapid and inexpensive way, and to create customised narratives for very specific audiences. It is important to note that digital technologies can be used both by the promoters of hybrid threats, to fabricate and spread disinformation, and the organisations that fight against them, to develop counter-narratives. In this chapter, both perspectives are considered.

The level of digital interconnectedness represents an enormous challenge when building an effective strategic communication to counter hybrid threats. More and more people are exposed to a constant flow of information due to the combination of advanced telecommunication infrastructure, intelligent devices and online services. In the field of telecommunication infrastructure, the rollout of 5G networks will significantly enhance internet connection speed and the number of connected devices, amongst other benefits. In such a scenario, written information and static images will be progressively substituted by high-quality videos, which will be much easier to send and share, as main vehicles for the transmission of information. Promoters of hybrid threats will be able to take advantage of the most advanced AI techniques to create sophisticated false videos, thus enhancing the impact of disinformation campaigns. Therefore, the combination of 5G networks, video sharing and artificial intelligence would pose a severe risk to any institution or individual that is the victim of a disinformation campaign. Communication strategies should consider these new risks and design effective measures to deal with them.

Protecting information is an essential prerequisite to controlling the message. Information leaks can severely damage any communication strategy. That is one of the reasons why the security of 5G networks has become an intense battlefield between Western countries and China, where some of the main providers of 5G network equipment are established. This issue, and those related to how other technological advances impact strategic communications, is explained in the following paragraphs.

Security and competition issues in the 5G network rollout

Few technological innovations have aroused as much expectation as the 5G communication standard. It allows data rates to be increased by up to 10 Gbps (between 10 and 100 times more than 4G and 4.5G

networks) and the number of connected devices per cell. It reduces latency (to 1 millisecond) and network energy consumption. It also improves spectrum efficiency and extends battery life in low-power devices (ETSI, 2019). These characteristics make 5G a quantum leap in the field of communication infrastructure, which is bound to revolutionise strategic sectors such as health (improving remote health care, including surgery), mobility (allowing the proliferation of self-driving cars) or industry (increasing monitoring capabilities in real time to improve the efficiency of industrial processes), amongst others. It will also have significant implications in online communications, as 5G standard will boost video consumption. Video traffic is forecast to grow around 30 % annually between 2019 and 2025. As a result, video traffic in mobile networks is expected to account for 76 % of total mobile data traffic in 2025 (Ericsson, 2019). Therefore, any communication strategy must take into account the growth of video formats as a way to transmit information, and should evolve in the same direction.

The development of 5G infrastructure is mainly led by two countries (USA and China), with security issues at the top of the list of concerns. Most of the infrastructure equipment providers come from both countries, with some exceptions like Nokia, Ericsson and Samsung. While numerous European telecommunication companies are relying on Chinese providers for deploying 5G systems, the US government has enacted specific regulations to impede Chinese companies (formally 'foreign adversaries') to sell 5G network equipment to US telecommunications operators, alleging risks to national security, given the potential existence of backdoors in such equipment that would allow the Chinese government to carry out surveillance activity (Executive Officer of the President, 2019).

In the European Union, Member States acted independently until 2019, although they felt pressure to ban Chinese 5G vendors from the US government (Grieger, G., 2019). For instance, in early 2020 Germany was debating whether the Chinese company Huawei should be banned as a provider of 5G infrastructure for German operators (Bennhold, K. & Ewing, J., 2020). On the contrary, France decided not to prohibit French telecommunications operators working with Chinese providers to deploy 5G networks (Vidalon, D., 2019). In Spain, telecommunications operator Telefónica awarded the deployment of part of its 5G core network to this Chinese company, although Telefónica intends to reduce its dependence on Huawei in the coming years (del Castillo, I., 2019).

In January 2020, the NIS Cooperation Group, established by the NIS Directive to improve coordination and information exchange on cybersecurity matters amongst Member States and the European Commission, launched the EU toolbox on 5G cybersecurity (NIS Cooperation Group, 2020). It includes the results of the EU coordinated risk assessment of 5G network infrastructure in each Member State and the means to address them. Following the launching of the EU toolbox, in the same month the European Commission published a Communication aimed at defining a common European approach regarding the security of 5G networks (European Commission, 2020b). Quoting the toolbox, the communication recommended that Member States restrict the participation of high-risk suppliers in the deployment of key assets of 5G networks, but without completely forbidding their participation in the 5G network rollout. The Communication also encouraged Member States to ensure that telecommunications operators follow a multi-vendor strategy to avoid the risks of depending on a single provider.

Also, in January 2020, the UK adopted an intermediate and more precise position. Telecom vendors classified as *high-risk*, like Huawei, were allowed to provide 5G network equipment, but with tight restrictions. They could not sell equipment for the core of the UK's 5G network, and could not provide more than 35 % of the equipment for other network functions (mainly the radio access network). Additionally, high-risk vendors were banned from selling equipment for critical national infrastructure (UK Government, 2020).

Telecommunications networks security is one of the main pillars where the success of strategic communications is based. Without securing basic communication infrastructure, impeding intrusions, surveillance and information theft, any other measure to counter hybrid threats would be useless. It is

therefore not surprising that control of the greatest innovation in the field of communication standards, 5G, is at the heart of the geopolitical struggle between the world's major economic powers, the US and China. This struggle is leading European countries towards a great dilemma, as the adoption of strict measures to secure network infrastructure (such as banning Chinese vendors) could notably increase the cost and delay the 5G network rollout (GSMA, 2019).

Artificial intelligence: technology to create and counter disinformation

If 5G network security is attracting the attention of policymakers around the world, artificial intelligence (AI) is another 'trendy' technological topic. AI-based tools can be used to carry out actions in each of the five traditional instruments of power: military, political, economic, civil and informational (Guilong, Y., 2019). In the military sphere, one of the main uses of AI is supporting operations by means of unmanned aerial vehicles (UAV), unmanned underwater vehicles (UUV) or self-driving military vehicles, as well as information and data management. In the other instruments of power, AI is basically focused on information management. AI is playing a double role in these spheres of power, as it can be used both by promoters of hybrid threats (for instance, carrying out disinformation campaigns by fabricating and spreading false content) and the attacked actors in order to counter them. Therefore, AI-based solutions will be key elements in creating counter narratives when developing communication strategies.

From the perspective of the promoter of hybrid threats, AI opens up new opportunities to develop more sophisticated attacks, as it contributes to creating more realistic fake content and improving its spreading, by profiling potential targets and increasing the accuracy of disinformation campaigns. Regarding the content, AI can be used to fabricate news without human intervention, which could accelerate and reduce costs of disinformation campaigns. For instance, OpenAI, a research laboratory based in San Francisco, has developed an unsupervised language model, called GPT-2, which can generate coherent paragraphs of text. However, as OpenAI stated, 'due to our concerns about malicious applications of the technology, we are not releasing the trained model' (Radford, A. et al., 2019). A tool of this kind could flood the internet with false information in a very short time.

AI does not only contribute to creating false written content. Audio and video content can also be manipulated through AI tools to create so-called *deepfakes*. Some notorious examples, including the manipulated video of Mark Zuckerberg talking about the control of Facebook users' data[14], or the proliferation of deepfake pornographic videos (Ajder, H. et al., 2019), some of which aim to destroy the victim's reputation, show their potential danger.

The spread of disinformation and propaganda can also benefit from the potential of AI. By processing the vast amounts of data that social media platforms have about their users, AI allows very detailed segmentations that can contribute to increasing the effectiveness of disinformation campaigns. Segmentation and microtargeting are recurrent marketing strategies that can also be used by promoters of hybrid threats to reinforce the impact of their campaigns. The Cambridge Analytica scandal is the best example of misusing AI-based segmentation techniques. This company collected personal data from millions of Facebook users without their consent and used this data to profile and segment the users into specific groups through AI tools. Some politicians, the best-known being 2016 US presidential elections candidates, Ted Cruz and Donald Trump, hired Cambridge Analytica's services, based on illegally harvested users' data, to influence voters' choices (Granville, K., 2018).

Along with segmentation, AI can also be used to amplify the impact of disinformation campaigns. AI bots are designed to simulate human behaviour on social media (for instance, commenting and replaying posts, using hashtags, etc.) in order to deceive human users and accelerate the spread of fake

[14] https://www.businessinsider.com/deepfake-video-mark-zuckerberg-instagram-2019-6?IR=T

content. They can also learn from previous situations to improve their outcomes (Center for Information Technology and Society - University California Santa Barbara, 2019).

According to the experts interviewed, AI techniques are not yet being widely used by promoters of hybrid threats to create and spread false information. Nowadays, attackers tend to rely on the easiest and cheapest means to reach their goals. However, as the cost of AI technology decreases, its use for malicious purposes will increase.

Artificial intelligence not only represents an opportunity for the development of hybrid threats. It is also a relevant technology for countering them, especially in the creation of detection tools. AI algorithms can evaluate and check news and accounts on social media to decide if they should be classified as *fake*. One example is the Grover AI model, developed by the Allen Institute for AI, which achieves over 92 % accuracy in classifying human-written and machine-written news (Allen Institute for AI, 2019). These algorithms are usually referred to as *Automated Content Recognition (ACR) technologies* (Marsden, C. & Meyer, T., 2019), and can act autonomously or as a supplement to human content moderation.

Although AI has the potential to help in the fight against the automated spread of disinformation, its use raises some ethical and legal concerns, mainly related to the ultimate responsibility of taking down contents or accounts classified as *fake* (as there could be false positives). Removing fake contents or accounts should be done in a way that preserves the right to freedom of expression, meaning human supervision will always be necessary (Marsden, C. & Meyer, T., 2019). A technology as disruptive as AI requires sufficient guarantees of its proper functioning. For that reason, proposals have been made for the application of mechanisms of Certification of Conformity aimed at ensuring the aforementioned guarantees (Galán, C., 2019).

Other technologies suitable for both creating and countering hybrid threats

There are other technological innovations that can act as a driver for the development of hybrid threats. One of them is the **Internet of Things (IoT)**. We are quickly moving towards a hyperconnected world, with multiple devices (home and medical appliances, cars, clothes, etc.) and sensors connected to the internet. A market research company has forecasted that there will be more than 41 billion connected IoT devices worldwide by 2025 (IDC, 2019). Thus, attack vectors grow exponentially and can be targeted towards very harmful actions against individuals or organisations. In such a scenario, network security will become a major issue, as potential cyberattacks could be more dangerous than ever before (ENISA, 2017). Some real-life examples of this great menace could be hacking insulin pumps or pacemakers or deliberately causing accidents with self-driving cars.

IoT technologies can also play a prominent role in the field of strategic communications. As described above, any communication strategy must first interpret reality, based on data and information. Based on this interpretation, narratives aimed at both informing or influencing targets and debunking attackers' visions of reality can be built. IoT technologies can contribute to developing coherent communication strategies by allowing collection of more data and information from the physical domain, which will aid better understanding what is happening before creating the appropriate narratives.

Blockchain technologies are the last technological hype that can collaborate in the fight against disinformation. In comparison with the most common types of communication platforms, blockchain-based systems provide enhanced security and allow traceability of the information recorded through its decentralised peer-to-peer functioning scheme. Although development of these technologies is still in its infancy, there is already some interesting academic research aimed at certifying the veracity of news using blockchain systems.[15] On a more practical level, the News

[15] (Qayyum, A. et al., 2019); (Huckle, S. & White, M., 2017); (Shang, W. et al., 2018)

Provenance Project,[16] launched by the New York Times Research and Development team, has suggested using blockchain technology to store contextual information about news photos (when, where and by whom they were taken, and how they have been used by news outlets) as a way to ensure the veracity of images in the media. In 2019, the New York Times developed a proof-of-concept of the technical solution proposed by that project, whose conclusions were expected for 2020 (Koren, S., 2019). Another relevant example of the use of blockchain to certify sensitive information can be found in Estonia. All official announcements and legislative documents published digitally in *Riigi Teataja* (the Estonian official public journal), as well as the President's speeches published online, are signed with blockchain technology in order to guarantee integrity and veracity (Krusten, M., 2019). This way, any manipulation of the information can be easily detected and rejected.

Blockchain will undoubtedly contribute to improve strategic communications by ensuring the veracity of information and helping to detect disinformation more quickly.

3.2.2. Influence of strategic communications on economic affairs

The economy is one of the fields that is most sensitive to the veracity and accuracy of information. Any false, incomplete or even vague news may lead to negative fluctuations in the stock market, may increase a country's risk premium, driving up the cost of its debt, or may deteriorate the credit score of a company, preventing it from accessing funding at a reasonable cost. Trustworthiness is an essential economic asset (Wilson, P. & Kennedy, A., 1999), so any hybrid threat, mainly in the form of disinformation campaigns, aimed at undermining it represents a serious risk for the economic system.

Disinformation attacks in the economic sphere can pursue diverse objectives. They may sometimes be part of a comprehensive strategy of destabilising the target. However, it is more common for attackers to seek their own economic benefit. An example of the first objective (general destabilisation with economic consequences) was the false news about explosions in the White House spread through Twitter in 2013. A tweet with the false information was sent out from the Associated Press account (one of the most reputed sources of information in the USA), which was hacked by the self-proclaimed Syrian Electronic Army in the context of the Syrian civil war. In a matter of minutes, this false information caused the momentary collapse of US stock markets and panic among investors. It was estimated that more than US$130 billion of S&P 500 index's value was wiped out before the market recovered (Selyukh, A., 2013).

There are also many examples of disinformation attacks pursuing economic benefit (Cheo, J., 2018). For instance, in 2015 the US Securities and Exchange Commission (SEC) filed securities fraud charges against a trader who spread false information about two companies on Twitter, using accounts that simulated those of reputed securities research companies. His intention was to artificially bring down the companies' stock price to buy shares and sell them after the price recovered, obtaining a large profit. The false tweets related to the two companies (Audience, Inc. and Sarepta Therapeutics, Inc.) caused their stock price to fall 28 % and 16 %, respectively (Securities and Exchange Commission, 2015).

Recent academic research showed that false information about a firm increases trading activity and stock price volatility compared to true information. Moreover, the study also concluded that the public revelation of the existence of disinformation causes an immediate decrease in activity on the stock market in reaction to all news, including the legitimate news, thus limiting their normal operation (Kogan, S. et al., 2019). Another study estimated the global annual losses caused by disinformation to the stock market at US$39 billion (Cavazos, R., 2019).

A coherent and coordinated communication strategy, aimed at building (or restoring) trust, is essential for the proper functioning of the economic system. One of the best examples of the impact of strategic communications on the economy was the famous 2012 discourse of the former President of the

[16] https://www.newsprovenanceproject.com/

European Central Bank, Mario Draghi, during the height of the Euro crisis (Draghi, M., 2012). When financial markets were relentlessly attacking the Italian and Spanish economies, causing unbearable increases in their risk premiums and questioning the viability of the Euro, only a few words ('the ECB is ready to do whatever it takes to preserve the Euro') managed to dispel doubts about its survival. Shortly after Draghi's discourse, the ECB announced diverse economic programmes to assist in the recovery of the weaker economies of the Eurozone, reinforcing Draghi's message. The impact of this communication strategy was so important that the words '*whatever it takes*' have become the preferred motto of the European leaders when managing the economic consequences of the Covid-19 crisis (Briançon, P., 2020).

3.3. National initiatives

After describing how strategic communications can contribute to countering hybrid threats from a theoretical perspective, this chapter is focused on showing practical implementations at the national level. The analysis conducted has revealed that so far, no country has implemented a holistic communication strategy that tackles all potential components of a hybrid threat. However, diverse countries have already implemented public initiatives leveraging specific aspects within the realm of strategic communications. The following paragraphs summarise the most relevant or novel policies and initiatives aimed at addressing concrete impacts of hybrid threats at the national level.

The US, pioneer in the use of the strategic communications concept

The United States can be considered the pioneer country in the definition of strategic communications. Since the Cold War era, the US has repeatedly highlighted the importance of having a coherent communication strategy, both from political and military perspectives, in order to spread its vision of a free and democratic world. The US vision regarding strategic communications has been consolidated during the last four decades in the diverse updates of its National Security Strategy (NSS). That vision has evolved in line with the threats the USA has faced and the means its enemies have used, from USSR interference at the end of the Cold War, to the War on Terror against extremist groups after the 09/11 attacks, and now again the Russian meddling in Western democracies.

Each new edition of the US NSS has focused on different issues related to strategic communications. The 1987 US National Security Strategy took into consideration the most relevant constituent components of strategic communications and how they had to be used to disseminate Western values and improve the reputation of the USA in the global context, which remained deeply damaged since the end of the Vietnam War (Baños, P., 2011).[17] In 2008, in the context of the War on Terror against extremist groups in Iraq and Afghanistan, the NSS recognised the need to improve coordination between the different departments and agencies across the US government to build effective strategic communications. In 2010, the NSS stressed the necessity of aligning actions and information.[18] The last

[17] In the National Security Strategy (NSS) of 1987, prior to the fall of the Iron Curtain, the US recognised that they were faced with 'a profound challenge to our national security in the political field. This challenge is to fight the war of ideas and to help support the political infrastructure of world democracies' (The White House, 1987, p. 13). The term *strategic communications* didn't appear in the 1987 NSS. They used instead the *political and informational strategy* concept, that 'must also reach the peoples of denied areas, particularly the USSR and Eastern Europe to encourage hope for change and to educate publics on the benefits of free institutions. This is achieved through the electronic media, written materials, and the increased contact and exchange of ideas that come from such contact… We must actively counter Soviet propaganda and active measures using the full range of U.S. informational programs' (The White House, 1987, p. 13).

[18] 'Effective strategic communications are essential to sustaining global legitimacy and supporting our policy aims. Aligning our actions with our words is a shared responsibility that must be fostered by a culture of communication throughout government' (The White House, 2010, p. 16).

edition of the US NSS, published in December 2017, focused on improving American influence through coherent communication campaigns.[19]

The recurrent inclusion of strategic communications as a key element of the National Security Strategy, the cornerstone of all security policies in the USA, highlights the political relevance of this concept in that country. The fact that strategic communications are being considered at the top political level reflects the theoretical concern about foreign influence, although practical implementation has not been able to avoid concrete cases such as Russian meddling in 2016 presidential elections.

Raising awareness amongst citizens in Sweden and Finland

As has been already analysed, strategic communications must be aimed at diverse kinds of targets, with different approaches. One of the targets is the population of the country defining the strategy. Citizens should be aware of the existence of disinformation campaigns aimed at influencing the society's normal development (for instance, polarising opinions on hot topics like migrants, nationalisms, etc.) and the political environment. Raising such awareness depends on massive educational initiatives and communication campaigns to allow citizens and specific groups to identify disinformation and limit its social influence. Within the European Union, two initiatives are worth mentioning: the role of the Swedish Civil Contingencies Agency in countering disinformation and the Finnish and Swedish government initiatives to educate citizens, students, journalists and politicians on how to detect disinformation (Hanlon, B. & Rosenberger, L., 2019).

The Swedish Civil Contingencies Agency (MSB in Swedish) was established by the Swedish government in 2009, combining the Swedish Rescue Services Agency, the Swedish Emergency Management Agency and the Swedish National Board of Psychological Defence (Cederberg, G., 2018). Although its initial mission was focused on the field of emergency management, after the Russian hybrid campaign against Ukraine in 2014-2015 its competences were expanded to deal with disinformation and foreign influence. In 2017, it was designated the primary authority for protecting the 2018 Swedish elections. In the context of these elections, the MSB developed several information campaigns to warn diverse collectives about potential foreign meddling. Regarding citizens, the MSB published and distributed a reviewed edition of the brochure *If Crisis or War Comes* (Swedish Civil Contingencies Agency, 2018a) to all Swedish households (around 4.7 million). This brochure explicitly mentioned disinformation and included easy instructions for all to deal with it. Thus, each Swede was informed about the potential existence of false information in order to reduce its influence in the elections. Another action, aimed specifically at the group of communicators working with public administrations, was the production of a handbook on countering information influence activities (Swedish Civil Contingencies Agency, 2018b). This handbook was intended to help communicators from public administrations to identify disinformation and prepare their organisations to manage responses. The publication of the handbook was complemented by training programs for over 10 000 public servants at the national, regional and local levels, to improve their ability to detect foreign influence campaigns (Cederberg, G., 2018).

In the field of education, both Sweden and Finland have implemented reforms in their national curriculums to increase the ability of children and young people to recognise false information.

Finland finished the deployment of its revised curriculum in 2016. The reform included new skills for all Finnish students directly linked to the ability to detect misinformation (FactBar EDU, 2018):

- Thinking and learning to learn;
- Cultural competence, interaction and self-expression;

[19] 'Drive effective communications: we will craft and direct coherent communications campaigns to advance American influence and counter challenges from the ideological threats that emanate from radical Islamist groups and competitor nations. These campaigns will adhere to American values and expose adversary propaganda and disinformation' (The White House, 2017, p. 35).

- Multiliteracy;
- Participation, involvement and building a sustainable future.

Based on these transversal competencies, the ultimate goal of which is to improve the critical thinking skills, fact-checking agencies such as FactBar[20] have created media and information literacy training programs for diverse educational levels to help students identify disinformation. The so-called *voter literacy toolkit* follows the recommendation included in the European Commission Communication *European approach to tackle online disinformation* that 'encourages independent fact-checkers and civil society organisations to provide educational material to schools and educators' (European Commission, 2018b).

In Sweden, the national curriculum was reformed in 2018 to increase computer science skills and the ability to detect false information amongst elementary and secondary school students (Cederberg, G., 2018). In this reform, institutions related to digital literacy and fact-checking, such as the Swedish Media Council, the Internet Foundation in Sweden, the Swedish Institute and the fact-checking initiative *Viralgranskaren* were involved. As in Finland, diverse educational toolkits were developed to foster critical thinking when accessing online information. One example is the Fake ≠ Fact toolkit, designed by the Swedish Institute.[21]

Both countries currently lead the *Media Literacy Index* (Finland ranked 1st position and Sweden 4th), which measures countries' resilience to disinformation (Lessenski, M., 2018).

Given the growing relevance of education to cope with disinformation, the OECD Program for International Student Assessment (PISA) has assessed, for the first time in 2018, students' capacity to distinguish between fact and opinion when reading about an unfamiliar topic. (Schleicher, A., 2019).

Raising awareness and coordination efforts to tackle online disinformation in Canada

In recent years Canada has implemented several initiatives to limit the effects of disinformation. From public programmes aimed at raising awareness to coordination strategies between governmental agencies, the Canadian initiatives can be considered a good, comprehensive communication strategy, although some components are still missing.

In 2019, the Canadian government launched the Digital Citizens Initiative, an ambitious strategy aimed at 'support[ing] democracy and social cohesion in Canada by building citizen resilience against online disinformation and building partnerships to support a healthy information ecosystem' (Government of Canada, 2019c). Through this strategy, the Canadian government finances diverse activities to improve the digital literacy of citizens (citizen-focused activities) and help them understand the impact of disinformation (Digital Citizen Research Program). The Digital Citizens Initiative as a whole can be considered within the realm of awareness-raising measures.

The activities focused on citizens take place as part of three programmes:

- Canada History Fund, which supports the production of learning materials and the organisation of learning activities related to the Canada's history. It aims to improve the Canadians' knowledge of their own history and values.
- Collective Initiatives – Canada Periodical Fund, which provides funding for projects that contribute to the sustainability of the Canadian magazine and newspaper industries.
- Youth Take Charge, which encourages young people to strengthen their bonds with Canada through arts and culture, civic engagement and other activities.

[20] https://faktabaari.fi/in-english/

[21] https://sharingsweden.se/toolkits/introducing-source-criticism-classroom/

The Canadian government invested US$7 million in 2019 to fund these programs (Canadian Heritage, 2019).

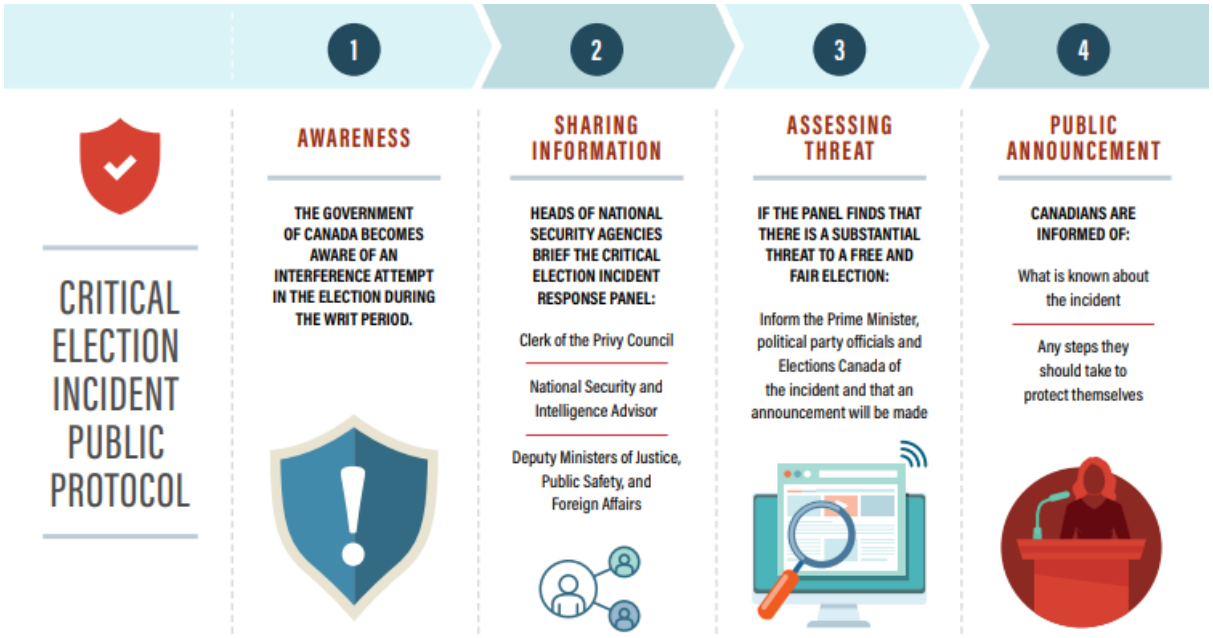
Regarding the Digital Citizen Research Program, it has three main components:

- Digital Citizen Contribution Program, which finances research projects to counter online disinformation in order to support democracy and social cohesion in Canada.
- Joint Initiative for Digital Citizen Research, which seeks to promote research activities to better understand how online disinformation is affecting Canadian society and which countermeasures can be applied, as well as supporting the Canadian research community on digital citizenship and online disinformation.
- Support to the Public Policy Forum's Digital Democracy Project, which brings together civil society, academia and political practitioners to discuss how to address the online disinformation.

The Canadian government has planned to invest US$19.4 million over four years to support the Digital Citizen Research Program (Canadian Heritage, 2019).

Another recent initiative from the Canadian government in the field of strategic communications has more to do with improving coordination between governmental agencies and bodies when tackling foreign influence. The Security and Intelligence Threats to Elections (SITE) Task Force was established in January 2019 to ensure a fair electoral process without foreign meddling (Hanlon, B. & Rosenberger, L., 2019). This task force included intelligence services, foreign policy bodies, law enforcement and cybersecurity agencies, working together to offer coordinated responses to foreign threats. Along with the SITE Task Force, the Critical Election Incident Public Protocol was established in July 2019. Its purpose was 'to ensure coherence and consistency in Canada's approach to publicly informing Canadians during the writ period about incidents that threaten Canada's ability to have a free and fair election' (Government of Canada, 2019b). The following image summarises the steps included in the protocol:

Figure 7: Critical election incident public protocol in Canada



Source: Government of Canada

Both the SITE Task Force and the Critical Election Incident Public Protocol can be deemed as good practices in the use of coordinated communications strategies to counter hybrid threats, in this case aimed at destabilising the electoral process.

An example of coordination to adjust management of strategic communications: Australia

Coordination between all stakeholders involved in responding to hybrid threats is an essential requisite of any communication strategy. The Australian government, being aware of the necessity of tackling foreign meddling in home affairs in a coordinated way, has carried out two main initiatives: the development of Australia's Counter Foreign Interference (CFI) Strategy and the creation, in April 2018, of the position of the National Counter Foreign Interference Coordinator (NCFIC).

The Australia's CFI Strategy is based on five principal pillars, aimed at 'enhancing capability, engaging with at-risk sectors, deterring perpetrators, defending against acts of foreign interference, and enforcing counter foreign interference laws' (Department of Home Affairs, 2019b). Two pillars are directly linked to strategic communications (*engage at-risk sectors to raise awareness and develop mitigation strategies* and *defend directly against foreign interference activity through a coordinated government response*).

However, the most relevant initiative, which highlights the importance placed on coordination in order to face hybrid threats by the Australian government, was the appointment of the NCFIC. The NCFIC is responsible for the coordination of diverse government agencies to assess the risks and consequences of foreign interference, the development of strategies to deter and prevent foreign interference, the implementation and management of Australia's Counter Foreign Interference Strategy and relationships with country allies to develop coordinated actions at the international level (Department of Home Affairs, 2019a). Although the tasks of detecting and assessing the risks, and defining countermeasures to cope with foreign interferences depends on different governmental bodies (the Australian Federal Police, the Australian Security Intelligence Organisation, the Department of Defence, the Department of Home Affairs and the Department of Foreign Affairs and Trade, amongst others), coordination under a single manager allows for more effective responses.

Collaboration between governments and tech companies in Germany and the US

If coordination between stakeholders is key to developing a coherent communication strategy, collaboration is no less important. Especially in the field of online disinformation, collaboration between governments and tech companies, owners of digital services such as social networks or video-sharing platforms, is crucial to hinder the spread of false information. Although some interesting examples can be highlighted, the collaboration between governments and tech companies can be considered so far as limited to electoral processes, one-way (from governments to tech companies), ad-hoc and reactive (Hanlon, B. & Rosenberger, L., 2019).

Diverse national governments have approached tech companies such as Facebook, Twitter or Google to involve them in the struggle against online disinformation during their electoral processes. For instance, Facebook took down tens of thousands of fake accounts before the German federal elections in 2017. In September 2019, members of several US federal agencies and governmental bodies met with representatives from Facebook, Google, Twitter and Microsoft to discuss collaborative approaches in order to prevent foreign interference through social networks and other digital services in the 2020 presidential elections (Isaac & Alba, 2019).

A comprehensive national strategy in countering hybrid threats: Lithuania's case

Lithuania, along with the other Baltic States, is one of the EU Member States most exposed to hybrid campaigns originating in Russia. These campaigns try to interference in and influence Lithuanian society, promoting social tensions and distrust in public institutions (Flanagan, S. et al., 2019). This fact has led the country to develop, particularly since 2014 after Russia's hybrid campaign against Ukraine,

a robust national defence strategy in which communication activities play a pivotal role. It includes measures at different levels (Bajarūnas, E. & Keršanskas, V., 2018):

- Political awareness and commitment, achieving a wide consensus on the importance of hybrid threats.
- Military readiness, ensuring a minimum allocation of national budgets to defence and restoring military service to increase citizens' involvement in defending the nation.
- Rapid reaction and establishment of crisis management mechanisms.
- Enhancement of resilience, establishing the National Cyber Security Centre and reducing energy dependence on Russia.
- Adopting clearer regulations.

Regarding strategic communications, Lithuania has implemented a holistic set of measures to countering disinformation, including:

1 'Enhancement of strategic communications capabilities (establishment of specialised subunits at the Ministry of Foreign Affairs, the Ministry of National Defence, the Armed Forces, intelligence institutions as well as other departments – e.g. the Ministry of Culture);

2 enhancement of society's awareness of informational warfare and propaganda;

3 preventing the dissemination of war and hatred propaganda' (Bajarūnas, E. & Keršanskas, V., 2018, p. 157).

Some specific measures are worth noting, as they represent good examples of society's engagement and international collaboration. For instance, some civil movements are taking responsibility for tackling hybrid threats through communication initiatives. The Lithuanian Riflemen Union, a paramilitary non-profit organisation, is actively taking part in patriotic education and civil resistance activities (Bajarūnas, E. & Keršanskas, V., 2018). The so-called *Lithuanian Elves* is an army of volunteers who fight online disinformation spread by Russian *trolls*. In the field of international collaboration, Lithuania is actively participating in information sharing and coordination platforms between the Baltic states, Nordic countries and Poland.

An example of public body exclusively focused on strategic communications: the UK Research, Information and Communications Unit

The Research, Information and Communications Unit (RICU), created in 2007, is a specialised unit within the National Counter Terrorism Security Office at the Home Office of the UK government. Its work is focused on countering terrorism and extremism, as well as organised crime (UK Government, 2017). Its most relevant characteristic is that the RICU's activities are aimed at challenging and countering extremist propaganda from terrorists' groups such as Al-Qaeda or ISIS amongst their targeted audiences (young British and non-British Muslims). The RICU produces and distributes online content (social network posts, videos, films, etc.) in order to influence online conversations amongst a specific target audience.

Although the RICU's work could be considered contentious, as it has been developed under the umbrella of the controversial counter-radicalisation programme called Prevent Strategy (UK Government, 2011), which has been repeatedly accused of not respecting human rights (Warrell, H., 2019), it is a clear example of the use of strategic communications to reach potential supporters of adversaries.

Legislative initiatives across the EU

The struggle against the communicational components of hybrid threats, mainly online disinformation, requires an appropriate legal framework. Some countries have recently endorsed new laws in order to protect their citizens and institutions from foreign interference through digital means, especially during electoral processes.

France has been one of the pioneer Western countries legislating to combat disinformation. After the terrorist attack at the Charlie Hebdo magazine offices, France approved the Decree no. 2015-125 of 5th February 2015, allowing French police authorities to block websites containing materials inciting terrorism or disseminating child pornography without a court order. In November 2018, the French National Assembly approved a new law to combat disinformation during electoral processes, which includes transparency obligations for digital platforms regarding sponsored ad campaigns and allows the French Broadcasting Authority to suspend foreign-controlled broadcasters that spread false news (Robinson, O. et al., 2019).

In Germany, the Act to Improve Enforcement of the Law in Social Networks (*Netzwerkdurchsetzungsgesetz* or NetzDG) entered into force in January 2018. Its main purpose is to engage online content distribution platforms (social networks, video platforms, etc.) in the fight against disinformation, making them responsible for taking down illegal contents under the German laws (Heidi T. & Leerssen, P., 2019). The law pursues crimes included in the Criminal Code such as dissemination of propaganda or symbols of unconstitutional organisations; incitement to hatred; dissemination of depictions of violence; defamation of religions; religious and ideological associations; public incitement to crime or breach of the public peace by threatening to commit offences, amongst others (European Commission, 2018f).

NetzDG obliges online platforms to create a procedure enabling users to report the existence of potential illegal content. After a report is made, the online platform must investigate whether the reported content is indeed illegal. If the content is *manifestly unlawful,* the platform must take the illegal content down within 24 hours. Other illegal content must be removed within 7 days. (European Commission, 2018f). Platforms that fail to comply with this requirement can be fined up to €50 million. German law also imposes transparency obligations for online platforms. If an online platform receives more than 100 complaints per calendar year about illegal content, it must produce a semi-annual report detailing how it has managed such complaints. Although the law received great support from German citizens, according to a poll conducted after its approval (Heidi T. & Leerssen, P., 2019), it has also been criticised by several collectives (tech industry, digital activists, civil rights activists, journalists) for 'jeopardising the core principles of free expression' (Digitale Gesellschaft, 2017).

Spain, in the context of the Catalonian conflict, passed a decree (14/2019 of 31st October 2019), allowing administrative authorities to intervene in telecommunication networks and electronic communication services, as well as to block potential illegal online activities, before a court order is granted, in the event of imminent and serious threats to public order or national security.

Regarding the spread of disinformation and hate speech through audiovisual media services, the Lithuanian Radio and Television Commission is legally allowed to temporarily ban programmes or channels with those objectives (Bajarūnas, E. & Keršanskas, V., 2018). On several occasions, the European Commission has supported Lithuania's decision to suspend broadcasting of the Russian language channel *RTR Planeta*, considering such decisions as compatible with EU rules, particularly the Audiovisual Media Services Directive, which forbids hate speech and incitement to hatred (a usual objective of disinformation campaigns).[22]

[22] C(2015) 4609 Final https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=10299

C(2017) 814 Final http://ec.europa.eu/newsroom/document.cfm?doc_id=42897

Legislative initiatives outside the EU

Outside the EU, two legislative reforms aimed at hindering foreign meddling can be highlighted: The National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (the EFI Act) in Australia and the Election Modernisation Act in Canada. The Australian EFI Act, approved in June 2018, amends the Criminal Code to introduce new, or modify existing, espionage offences related to managing information, as well as new offences related to foreign interference. It also introduces new crimes related to national security such as interference with Australian democratic or political rights (Parliament of Australia, 2018). In addition to the Criminal Code, the EFI Act amends many others Australian laws (Australian Citizenship Act 2007, Australian Federal Police Act 1979, Commonwealth Electoral Act 1918, Foreign Evidence Act 1994, Migration Act 1958, Surveillance Devices Act 2004, among others) to create a modern legislative framework that allows Australia to properly cope with foreign influence.

The Canadian Election Modernisation Act (EMA) entered into force in June 2019. The EMA is focused on preventing foreign influence in electoral periods by means of:

- prohibiting the use of foreign funds to pay for advertisement campaigns that attempt to influence elections;
- clarifying offences related to publishing of false statements aimed at interfering with election results;
- obliging online platforms to maintain and publish a registry of partisan advertising before and during the electoral period (limited to a maximum of 50 days).

These legislative reforms show alternatives ways to approach the communicational component of hybrid threats (the use of online platforms for spreading disinformation and foreign propaganda, mainly during election periods).

Improving the country's image: the case of the *España Global* strategy in Spain

In 2012, still suffering the effects of its major economic crisis, the Government of Spain established the High Commission of the Government for the *Marca España* (Spain Brand), with the objective of improving the image of Spain abroad and promoting the coordinated action of all institutions committed to 'Spain's interests in the economic, cultural, social, scientific and technological fields' (Government of Spain, 2012, p. 1). In practice, *Marca España* had a clear focus on strengthening the country's reputation as a key competitive factor for the Spanish economy and companies, as part of Spanish economic diplomacy.

In October 2018, one year after the illegal referendum on the independence of Catalonia, and four months since a new Government took office, the High Commission for the *Marca España* was transformed into the State Secretariat for Global Spain (Government of Spain, 2018). Although the overall objective of the institution did not formally change in substance (it is 'responsible for the management of Spain's image and reputation' (Ministry of Foreign Affairs, European Union and Cooperation, 2018)), the strategic shift was very clear. Its main objective was to improve the country's image not only abroad, but also amongst Spanish citizens themselves, in clear response to the attacks on Spain's reputation carried out by the Catalan independence movement and some populist groups.

The regional Catalan government had used strategic communications for nation-building purposes in Catalonia since 1979 (García-Muñoz, C., 2018). In addition, the efforts made by the Catalan pro-independence forces to internationalise the conflict intensified attacks on Spain's reputation,

C(2018) 2665 Final http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52093

spreading doubts about the quality and solidity of its democratic institutions and culture, especially in the run-up to the illegal referendum in 2017.

España Global's (Global Spain) strategy hinges on two fundamental pillars: coordinating external communication instruments and monitoring the messages disseminated about the country. To this end, it has developed arguments to counteract any negative messages, reinforced its strategy on social networks and launched a communication campaign called *This is the Real Spain*.

This is the Real Spain was created as a blog to 'spread the word about the real Spain, with its strengths and challenges within and outside our borders. Readers can find these strengths classified into three main pillars: democracy, modernity and citizenship' (Global Spain, 2018). The campaign included a video with relevant and internationally influential Spanish personalities.

In its aim of coordinating messages and provide foreign action with tools to counter attacks on the country's reputation, the body collects and disseminates evidence on positive aspects of Spanish culture, language, society or institutions, and has produced two reports: *The truth about the Catalonia's bid for independence* (Global Spain, 2019b) and *Spain: a global actor in the fight against climate change* (Global Spain, 2019a), in the context of the Spanish offer to hold the 25th Conference of the Parties (COP) of the United Nations Framework Convention on Climate Change (UNFCCC), which was originally to be held in Chile.

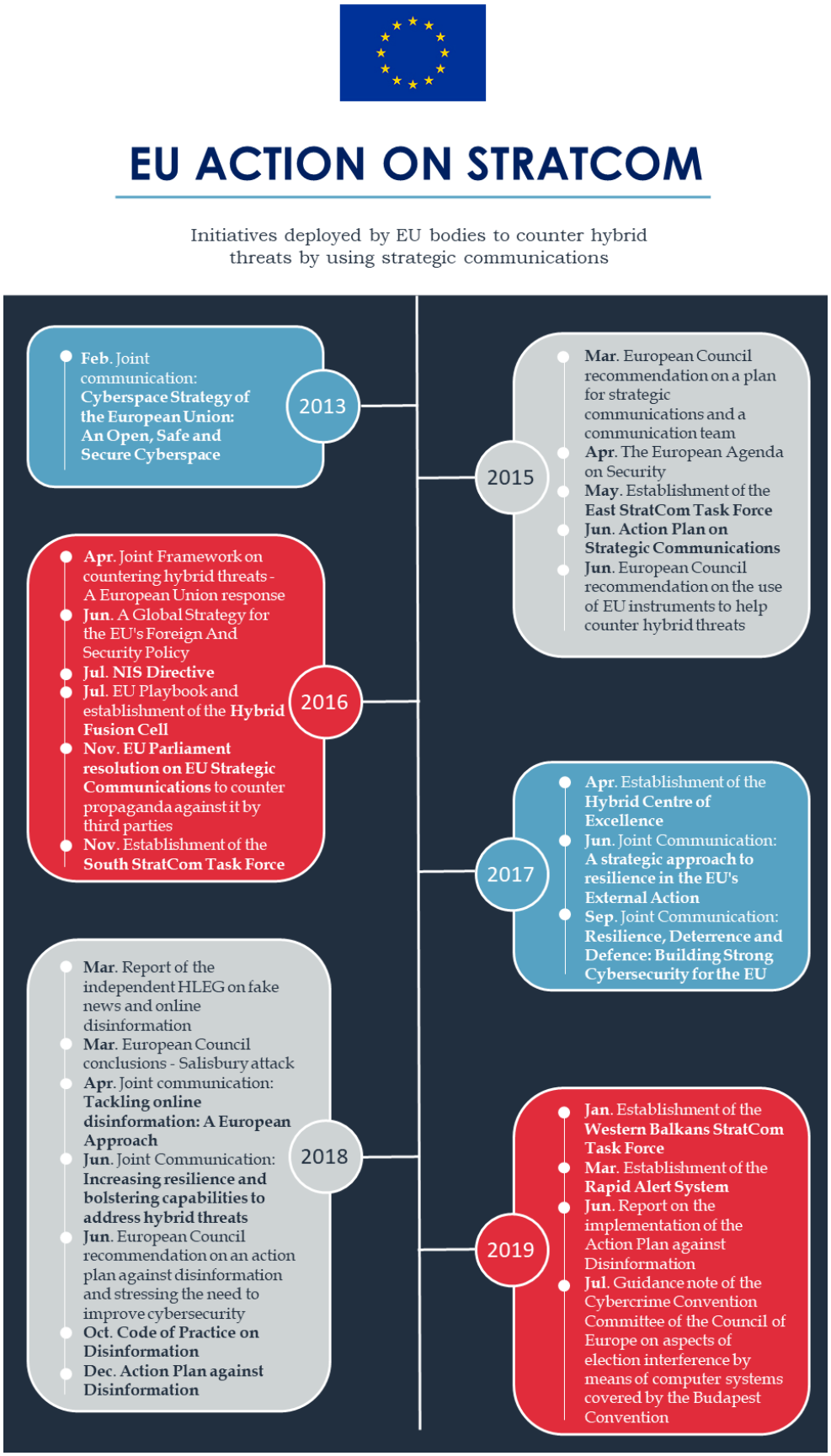
3.4. Initiatives from international bodies

Combating hybrid threats is not only taking place at the national level. Diverse international bodies are proposing strategies to counter them at different levels, including communicational responses, relying on international cooperation. This section will focus on the work done so far by the European Union, as well as other institutions like NATO or the G7. Thus, we get an overview of the current guidelines and the gaps that should be covered to set up a coherent and comprehensive strategy at the international level.

3.4.1. EU efforts to tackle hybrid threats

In recent years, the European Union has carried out intense activity to address the issue of hybrid threats. The following image summarises the main milestones of EU's activity:

Figure 8: EU actions to counter hybrid threats



Source: own elaboration

The main EU actions against hybrid threats related to strategic communications are the following:

2013

In 2013, EU concerns about hybrid threats were focused on cybersecurity. In order to address this threat, the European Commission released a Joint Communication including a roadmap for action in the immediate future, to ensure the development of a Network and Information Security policy. In this document, the first signs of strategic communication can be found. On these matter, the communication tasked the High Representative of the Union for Foreign Affairs and Security Policy, Member States and European institutions with facilitating dialogue around the application of international law in cyberspace, along with developing public guidelines to promote fundamental rights such as freedom of expression and access to the internet. (European Commission, 2013).

2015

In March, the European Council's conclusions recommended an action plan on strategic communication in order to challenge Russian disinformation campaigns (European Council, 2015). Two months later, the **East StratCom Task Force** was created within the EEAS (European External Action Service) to promote better communication of the EU policies, fight against disinformation campaigns and improve free and independent media in eastern countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine). Promptly, the East StratCom released the **Action Plan on Strategic Communication** in collaboration with other EU Institutions and Member States. The document contains the main guidelines of the StratCom team in Eastern Europe:

- Increase EU Strategic Communication capacity;
- work with partners and develop networks;
- communication activities on EU funded programmes, projects and activities in the Eastern Neighbourhood;
- support for freedom of the media and freedom of expression;
- public diplomacy initiatives in the neighbourhood;
- capacity building for journalists and media actors;
- supporting pluralism in the Russian language media space;
- engagement with civil society;
- increase awareness, develop critical thinking and promote media literacy;
- strengthen cooperation on regulatory issues in EU Member States (East StratCom Team, 2015).

2016

2016 could be described as the year in which hybrid threats were established as one of the main concerns for EU security. In April, the European Commission published an ambitious communication with an extensive framework for countering hybrid threats in the EU. Within its 22 actions, the communication includes one directly concerning strategic communication: 'The High Representative will explore with Member States ways to update and coordinate capacities to deliver proactive strategic communications and optimise the use of media monitoring and linguistic specialists' (European Commission, 2016a, p. 5).

In June, the European External Action Service released the document **A Global Strategy for the European Union's Foreign and Security Policy**. Strategic communications are considered one of priorities of external action, as a way to improve the EU's capacity to communicate its principles and

actions and, also, to 'offer rapid, factual rebuttals of disinformation' (European External Action Service, 2016b, p. 23).

In July, the European Parliament published the **NIS Directive**, aimed at improving the common level of cybersecurity in the EU. Among other instructions, Member States must have a CSIRT (Computer Security Incident Response Team) to counter cyberattacks. Regarding strategic communications, the NIS Directive creates a CSIRT network to connect Member States' CSIRTs and EU organisations (CERT-EU, ENISA) in order to promote effective cooperation in cybersecurity matters. The directive also establishes the NIS Cooperation Group in order to 'support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them' (European Parliament, 2016c, p. 17).

Almost at the same time as the NIS Directive was enacted, the European Commission released the **EU Playbook**, an operational protocol for countering hybrid threats between Member States, the Commission itself and the High Representative. Within this protocol, it is worth mentioning the creation of the **EU Hybrid Fusion Cell**, whose main task is to receive information and produce intelligence related to hybrid threats, to inform decision-makers in EU institutions and Member States. The protocol also defined EU crisis management procedures (European Commission, 2016b).

In November, the European Parliament published a resolution on **EU strategic communication to counteract propaganda against it by third parties**. The document pointed Russia, ISIL/Daesh and Al-Qaeda as the main informational threats using propaganda in the EU. The resolution considered strategic communication as a priority and encouraged responding to these threats with an offensive (instead of defensive) strategic communication. It also called on EU institutions and partners to coordinate a common strategic communication with both internal and external scope. In addition, the resolution established the **South StratCom Task Force**, also known as the Arab StratCom Task Force. (European Parliament, 2016d).[23]

2017

In April, the **European Centre of Excellence for Countering Hybrid Threats** was established in Helsinki. This centre was suggested by the European Commission and the High Representative in the aforementioned Joint Framework on countering hybrid threats. The Hybrid CoE was conceived as a research centre on hybrid threats, where EU Member States and partners (mainly NATO) could share knowledge and experience on this kind of issue (Council of the European Union, 2016).

In June, the Commission and the High Representative published the joint communication **A Strategic Approach to Resilience in the EU's external action**. The communication recalled the central role of strategic communications for strengthening state and societal resilience and suggested specific measures such as reinforcing the activity of Tasks Forces by increasing their resources (European Commission, 2017a).

Later, in September, the European Commission and the High Representative announced the **reform of ENISA** (European Union Agency for Network and Information Security) to extend its competences and tasks. The joint communication **Resilience, Deterrence and Defence: Building strong cybersecurity for the EU**, following the NIS Directive, stressed the necessity of building resilience through rapid emergency response mechanisms as well as 'awareness-raising in relation to online disinformation campaigns on social media' (European Commission, 2017b, p. 12).

[23] Its role was redefined in 2019, while a new one task force was created: Task Force for Western Balkans. (European Parliament, 2019).

2018

In 2018, the fight against hybrid threats focused on disinformation. In January, the Commission organised a High-Level Group of Experts (HLEG) on Fake News and Disinformation, whose task was to advise the Commission and the EU on those matters. In March, the HLEG released the report **A multi-dimensional approach: report of the independent High-Level Group on fake news and online disinformation**. The report recommended a set of measures and concrete actions to counter the threat of disinformation, which could be taken into account in the upcoming communication being produced by the Commission. All were related to strategic communications: defining a multi-stakeholder Code of Practice for fighting disinformation on social media; supporting media and information literacy for all citizens; supporting media innovation projects to empower journalists in dealing with disinformation, amongst others (High Level Group on fake news and online disinformation- European Commission, 2018).

In March, the European Council also reported its conclusions on the Salisbury chemical attack. The Council encouraged the European Union and Member States to improve their capabilities to face hybrid threats by means of strategic communications (European Council, 2018a).

In April, following the HLEG publication, the Commission released the communication **Tackling online disinformation: a European Approach**. This document highlighted the importance of strategic communication in tackling disinformation campaigns, emphasised the work already done (East StratCom Task Force, Hybrid Fusion Cell, Hybrid CoE) and proposed new tools to counter disinformation (creation of an independent European network of fact-checkers, launching a secure European online platform on disinformation, leveraging the Horizon 2020 work programme to support research on technologies such as artificial intelligence, blockchain, etc., amongst others) (European Commission, 2018b).

In June, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy reviewed the EU policies and actions on countering hybrid threats through the joint communication **Increasing resilience and bolstering capabilities to address hybrid threats**. Regarding strategic communications, the document stressed the necessity of improved coordination and cooperation across EU institutions, Member States and other partners, highlighting the importance of safeguarding election periods from cyberattacks (European Commission, 2018e).

In the same month, the European Council invited the High Representative and the Commission to put together an action plan against disinformation in cooperation with Member States, and to prepare the StratCom teams with appropriate mandates and resources (European Council, 2018b)

In September, the **EU Code of Practice on Disinformation**, proposed by the HLEG on disinformation and fake news and mandated by the Commission in the aforementioned communication[24] was published. It was signed by Facebook, Google, Twitter, Mozilla and other advertising companies in October. Microsoft joined the signatory companies in May 2019 (European Commission, 2019b).

In December, the High Representative and the European Commission released a joint communication containing an **Action Plan against Disinformation**, following the recommendations proposed in the communication on tackling online disinformation. It was motivated by the growth of disinformation strategies and the proximity of the European Parliament election (2019), plus more than 50 elections that were to take place in the EU by 2020. The measures of the plan were organised in four main pillars. The first was improving capabilities to detect, analyse and expose disinformation (the main proposed action for this purpose was to provide StratCom teams, Union Delegations and the EU Hybrid Fusion Cell with additional and specialised staff). The second pillar was strengthening coordinated and joint responses to disinformation, by means of setting up a **Rapid Alert System** (finally launched in March

[24] Tackling online disinformation: a European approach.

2019) and contact points for coordination amongst Member States. The third pillar was aimed at mobilising private sector to tackle disinformation, and the fourth was related to raising awareness and improving societal resilience (European Commission, 2018h).

2019

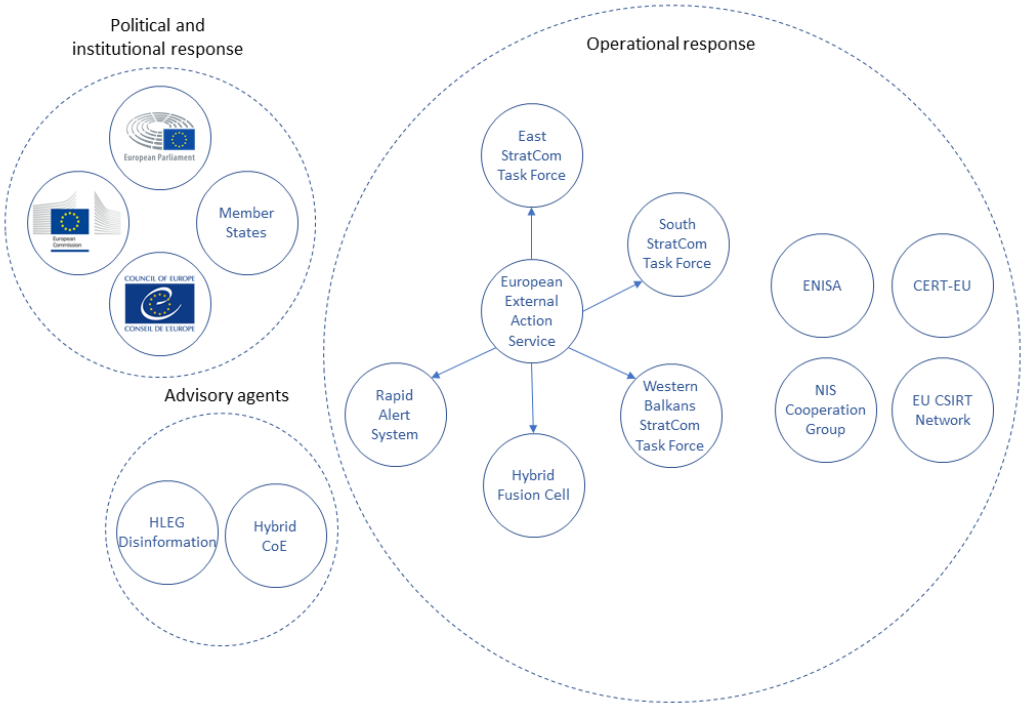
In June, the Commission and the High Representative published the first report on the implementation of the Action Plan against Disinformation, summarising the work done on the four pillars described above (European Commission, 2019c).

In July, the Cybercrime Convention Committee (T-CY), which represents the members of the Convention of Cybercrime of the Council of Europe, known as the Budapest Convention, adopted the **Guidance Note #9 Aspects of election interference by means of computer systems covered by the Budapest Convention**, noting that 'interference with elections through malicious cyber activities against computers and data used in elections and election campaigns undermines free, fair and clean elections and trust in democracy […] Domestic election procedures may need to be adapted to the realities of information society, and computer systems used in elections and related campaigns need to be made more secure' (Cybercrime Convention Committee (T-CY), 2019, p. 3). This guidance note was aimed to analyse how the Budapest Convention might be applied to prevent the impact of cyberattacks in electoral processes.

EU bodies specialised in strategic communications to counter hybrid threats

The EU's aforementioned activities focused on tackling hybrid threats have materialised in the creation of diverse bodies, which address this issue from different perspectives. The following image depicts the main stakeholders responsible for managing strategic communications applied to countering hybrid threats at the EU level.

Figure 9: EU bodies to combat hybrid threats



Source: own elaboration based on (Fiott, D. & Parkes, R., 2019)

3.4.2. NATO initiatives for leveraging strategic communications to counter hybrid threats

NATO is one of the most active intergovernmental institutions in the application of strategic communications as a tool to counteract hybrid threats. The first time NATO's leaders recognised the relevance of strategic communications was in April 2009, during the celebration of the 60th anniversary of the Alliance at the Strasbourg/Kehl Summit. The Summit Declaration stated, 'Strategic communications are an integral part of our efforts to achieve the Alliance's political and military objectives' (NATO, 2009a).

The overarching framework under which all of NATO's strategic communication activities have been designed is the NATO Strategic Communications Policy (NATO, 2009b), launched in September 2009 to deal with the increasingly complex operational and informational environment. However, there were intense debates and discrepancies within the Alliance on how to translate the overall strategy to specific activities (Laity, M., 2018). Only after the Russian aggression against Ukraine, where Russia used massive disinformation campaigns to influence diverse targets (civilians, Ukrainian soldiers, public servants, politicians, etc.), did NATO become truly aware of the importance of the informational responses to hybrid threats. In the declaration after the 2014 Wales Summit, NATO's leaders stated 'We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats […] It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces. This will also include enhancing strategic communications' (NATO, 2014).

One of the major steps to boost strategic communications as an effective tool against hybrid threats was the creation of the NATO StratCom Centre of Excellence in 2014, based in Riga, Latvia. The NATO StratCom CoE is aimed at providing 'a tangible contribution to the strategic communications capabilities of NATO, NATO allies and NATO partners' (NATO StratCom CoE, 2020b). This contribution is materialised in the design and development of training and education programs, research on how to effectively apply strategic communications, analysis of the lessons learnt regarding communication during NATO operations and dissemination of NATO doctrine on strategic communications. The StratCom CoE was accredited by NATO as an international military organisation in September 2014 and it does not directly depend on any NATO unit.

NATO strategic communications have been focused on the following domains:

Table 6: NATO strategic communications' domains

Public Diplomacy	Public Affairs	Military Public Affairs	Information Operations	Psychological Operations
NATO civilian communications for promoting awareness and building understanding and support for NATO's policies, operations and activities	NATO civilian engagement through the media to inform the public of NATO policies, operations and activities	Promoting NATO's military aims and objectives to audiences in order to enhance awareness and understanding of military aspects	NATO military advice and co-ordination of military information activities in order to create desired effects on the will, understanding, and capabilities of adversaries	Planned psychological activities using communication methods and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour

Source: (NATO StratCom CoE, 2020a)

3.4.3. Other intergovernmental initiatives

Diverse intergovernmental entities are implementing new mechanisms aimed at improving coordination and effectiveness of communication actions. One example is the G7 Rapid Response Mechanism (RRM), created by the G7 countries in 2018 after the annual meeting which took place in Charlevoix (Canada). The G7 countries issued the Charlevoix Commitment on Defending Democracy from Foreign Threats, where they committed to 'establish a G7 Rapid Response Mechanism to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, through sharing information and analysis, and identifying opportunities for coordinated response' (G7, 2018). The RRM is managed by a coordination unit within the Canadian governmental agency *Global Affairs Canada*. The coordination unit is responsible for sharing information between the G7 partners, analysing potential threats and coordinating responses when attacks occur (Government of Canada, 2019a).

The United Nations also has a Strategic Communications Division, whose mission is ensuring that UN communications campaigns achieve their goals. This division coordinates a global network of 60 UN information agencies.

4. Description of case studies

After analysing the concepts of hybrid threats and strategic communications from a theoretical perspective, this chapter addresses the study of these phenomena by presenting some recent examples. Seven case studies of actual manifestations of hybrid threats, and how the victims have leveraged communication strategies to implement their response, have been selected for analysis.

The following aspects have been considered in each case study:

- **The reasons** why the case study can be considered an example of hybrid threat.
- **The goals** pursued by promoters of hybrid threats: destabilise the target, spread their political vision or ideology, exploit target vulnerabilities (economic, social, technological), etc.
- **The strategies** implemented by perpetrators of hybrid threats to achieve their goals: disinformation campaigns through digital means, cyberattacks, covert military operations, economic or diplomatic pressure, etc.
- **The response** to the hybrid threat by the targets, particularly those related to strategic communications: creation of alternative narratives, development of fact checking mechanisms, economic sanctions, diplomatic pressure, review and reinforcement of security strategies (particularly related to cybersecurity), revaluation of risks posed by the hybrid threats, etc.
- **Lessons learned** by the targets after suffering the hybrid threat.

Cases have been selected to fully reflect all the components and essential characteristics of hybrid threats according to the most accepted definitions[25] and to include responses in the field of strategic communications.

The most paradigmatic case, which encompasses most of the features of hybrid threats, is the Russian attacks against Ukraine. This case has been included as the best example of hybrid threat in recent few years. Additionally, four cases from the NATO compendium of cases *Hybrid Threats: A Strategic Communications Perspective* (NATO StratCom CoE, 2019), which include new (or enhanced) hybrid mechanisms and innovative response measures based on strategic communications compared to those used in the illegal annexation of Crimea by Russia, have been included. The selected cases are the following:

- Rise of religious extremism in The Netherlands due to financing and support of the Salafi movement by the Gulf monarchies.
- Saudi Arabian pressure on Pakistan in the context of the civil war in Yemen.
- Foreign influence of Russia and China through academic institutions and think tanks.
- Russian electronic warfare during Zapad 2017 military exercises.

Finally, two recent cases that have drawn the attention of policymakers and geopolitical analysts about the danger that hybrid threats represent for EU countries and the necessity of developing good strategic communications at the highest level have been analysed:

- Disinformation campaigns against NATO operations in Lithuania.
- Disinformation attacks in the Catalan conflict.

[25] See Chapter 2.1

The selection of these cases allows examination of the implementation of all components that may be part of a hybrid threat and all potential countermeasures described in Chapters 2.1.1 and 3.2. From this, we can obtain useful insights about the evolving nature of hybrid threats and the instruments used to counter them from a practical perspective.

The following table summarises the components of hybrid threats and the countermeasures adopted in each case.

Table 7: Summary of the case studies

Case study	Hybrid threat components	Target's strategies to counter the hybrid threat
Rise of religious extremism in The Netherlands due to financing and support of the Salafi movement by the Gulf monarchies	Financing Salafist activities (building mosques and cultural centres, training radical preachers and imams). Salafist afterschool education. Spreading Salafist ideology through social networks.	Creation of alternative narratives to avoid radicalisation. Monitoring hate speech in social networks. Reinforcing cooperation with the Muslim community.
Saudi Arabian pressure on Pakistan in the context of the civil war in Yemen	Economic pressure of Saudi Arabia over allies. Religious influence of Saudi Arabia over allies. Diplomatic pressure.	Diplomatic measures (Pakistan´s neutrality). Searching for new economic allies (China).
Foreign influence of Russia and China through academic institutions and think tanks	Spreading Russian and Chinese political vision. Influencing academic production in foreign countries. Developing alternative narratives for historical events.	Raising awareness about the real nature and purposes of those academic institutions. Reforming the funding of academic institutions controlled by foreign countries, increasing transparency.
Russian intervention in Ukraine	Economic pressure. Covert military actions: annexation of Crimea and war in the Donbass region. Use of a legal narrative to justify the intervention. Cyberattacks. Disinformation campaigns. Religious influence.	Diplomatic pressure. Economic sanctions. Launching fact checking platforms to counter Russian disinformation.
Disinformation campaigns against NATO operations in Lithuania	Disinformation campaign based on false events.	Quick police investigation. Leveraging citizens' awareness to reduce the impact. Good communication strategies and coordination between all parties involved (Lithuanian authorities, NATO and German Army).
Russian electronic warfare during Zapad 2017 military exercises	Electronic warfare elements affecting diverse regions in foreign countries. Intimidation and coercion over neighbouring countries.	No measures were implemented as the details of the electronic attacks were discovered too late.
Disinformation attacks in the Catalan conflict	Foreign influence. Disinformation campaigns using bots in social networks. Use of social influencers to spread disinformation.	Creation of new public bodies to combat disinformation and cyberattacks. Revision of the national cybersecurity strategy to include disinformation as a real threat.

		Communication strategy to counter independentist narrative, developed by the Spanish Government.

Source: Iclaves

4.1. Case 1: Rise of religious extremism in The Netherlands due to financing and support of the Salafi movement by the Gulf monarchies

Since the beginning of the century, Dutch authorities have warned of the growing influence of extremist branches of Islam among Dutch Muslims. One of those branches, the Salafi movement, which advocates for a more rigorous interpretation of the Quran and Sunnah, is allegedly being promoted by Gulf States (General Intelligence and Security Service, 2019). Although the Salafi movement and its promoters do not intend to attack Dutch democracy as a specific and direct objective, it could lead to the radicalisation of some Muslims, especially young people. In turn, this could result in the growth of intolerant and antidemocratic attitudes that undermine social cohesion and threaten the proper functioning of Dutch democratic institutions. In particular, Salafist radicalisation, and its most extreme form, jihadism, has played a direct role in the increasing number of Dutch individuals who have fought under the orders of terrorist organisations like the Islamic State. According to official estimations, between 2012 and November 2018 more than 310 individuals travelled from the Netherlands to Syria and Iraq to combat for the Islamic State, 85 of whom were killed and 55 are estimated to have returned. Approximately 35 would have disappeared from the conflict areas. Thus, about 135 Dutch individuals continued fighting in 2019 in those conflict zones (General Intelligence and Security Service, 2018). This same source estimates that the Dutch jihadist movement is made up by of more than 500 supporters and several thousand sympathisers, which represents a serious domestic threat to Dutch society. Since 2013, the threat level in the Netherlands has ranged from 3 to 4 on a scale of 1 to 5, with occasional raises to level 5, for instance, after the tram attack in Utrecht on 18th March 2019 (National Coordinator for Security and Counterterrorism, 2019).

This case, therefore, constitutes an example of a hybrid threat in which foreign actors (in this case some Gulf monarchies) promote a religious belief (which is also intends to modelling social and economic behaviours) that could collide with European democratic values and exacerbate social tensions and polarisation in an EU country.

4.1.1. Geopolitical context

According to the Pew Research Centre (2017), in 2016 Muslims accounted for 7.1 % of the total population in the Netherlands, becoming the EU country with the fifth largest percentage of Muslim citizens after Bulgaria (11.1 %), France (8.8 %), Sweden (8.1 %) and Belgium (7.6 %). In the whole EU, Muslims accounted for 4.9 % of the total population. In absolute terms, the Muslim population in the Netherlands was estimated at 1.2 million people.

Muslim migrants began to arrive to the Netherlands in the 1960s, 1970s and 1980s. The main countries of origin were Morocco and Turkey (Hoorens, S. et al., 2015). Migration from Muslim countries has been constant in recent decades, with a relevant increase in recent years due to the Syrian civil war (Damhuis, K., 2019). Thus, the current Muslim population in the Netherlands is shaped by the second and third generations of descendants of the first migration wave in the previous century, and newcomers (mostly asylum seekers) from conflict areas such as Syria, Afghanistan or Libya, amongst others.

Most Dutch Muslims are followers of the Sunni doctrine. Within Sunni Islam, the Salafi intellectual current is considered one of the most conservative Islamic ideologies. Salafism seeks a return to the pure and true Islamic faith practised in the times of the Prophet Mohammad, basing social and economic relations on Sharia law. Salafists advocate a literal interpretation of the Quran and reject all

attempts to adapt Islam to modernity. In consequence, they do not consider democracy as the best way of ruling society (General Intelligence and Security Service, 2010). However, it is not a monolithic movement, as it encompasses diverse groups, from non-violent devotees, who are integrated into and live peacefully in Western countries, to Salafi jihadism, whose main example is the recently defeated Islamic State (Center for International Security and Cooperation - Stanford University, 2019).

Salafism, as an expression of the Wahhabi current of Islam, has been actively promoted by Gulf States such as Saudi Arabia since the 1970s (Hoorens, S. et al., 2015). Those countries have financed the spreading of Salafi movements around the world, creating international Salafi networks as well as supporting local branches.

4.1.2. Features of the hybrid threat

Since the late 2000s, Salafism has attracted Dutch political attention as a potential threat to democratic values and social cohesion. The most recent crises in the Middle East (the Syrian civil war) and North Africa (the Arab Spring and the subsequent power gaps in some Maghreb countries), as well as the religious influence exerted by foreign countries like Saudi Arabia or Kuwait, triggered concerns in countries with relevant Muslim minorities such as the Netherlands (General Intelligence and Security Service, 2015).

Promoters of Salafism, mainly Saudi Arabia, Kuwait and other Gulf States, seek to spread this radical interpretation of Islam amongst Muslims around the world. Although at a first sight this strategy could be considered a merely religious goal, it has important societal and political implications, given that Salafists do not only consider Islam as a faith, but also as a political system (ruled by the Sharia law). Thus, the radicalisation of Dutch Muslims by embracing Salafism could lead to a deterioration of the democratic legal order in the Netherlands (General Intelligence and Security Service, 2015). Salafism rejects democracy as a political system, so its supporters may consider it both legitimate and necessary to act to undermine it from within, using undemocratic methods. The risk of a direct or indirect involvement of Salafist radicals in violent actions and terrorist activities must also be considered (NATO StratCom CoE, 2019).

The means used to spread Salafism in the Netherlands are diverse. One of the most relevant has been financing the construction of mosques, cultural centres and organisations throughout the whole country, many of which are financed by foreign sources. For example, in 2018 a list of at least 30 Dutch Islamic organisations that had received funding from Kuwait and Saudi Arabia since 2010 was revealed (Holdert, M. & Kouwenhoven, A., 2018). While some funds came from charities and NGOs, others were directly provided by government departments like the Ministry of Awqaf and Islamic Affairs in Kuwait.[26] This ministry aims to spread Islamic culture and 'contribute to the development of society in accordance with Islamic understanding, reality and realisation' (Ministry of Awqaf & Islamic Affairs, n.d.). One of the charities that funded Dutch Islamic organisations was the Revival of Islamic Heritage Society, which was included on the Al-Qaida Sanctions list by the UN in 2002 (United Nations Security Council, 2014). Although the direct participation of Gulf governments in charities that fund Western Islamic institutions is difficult to prove, given the opacity about their financial sources, there are some cases that seem to confirm it. For instance, the *Blauwe* Mosque in Amsterdam received €400 000 from the Ministry of Awqaf and Islamic Affairs in Kuwait through an intermediary foundation, the European Trust Network (Hoorens, S. et al., 2015, p. 16). Salafist mosques have been accused of 'propagating an intolerant, isolationist and antidemocratic message' (General Intelligence and Security Service, 2015, p. 7). According to the National Coordinator for Security and Counterterrorism, the number of Salafist

[26] http://download.omroep.nl/nos/docs/lijst-Koeweit-1.pdf
http://download.omroep.nl/nos/docs/lijst-Koeweit-2.pdf
http://download.omroep.nl/nos/docs/lijst-Saoedi-Arabie.pdf

mosques in the Netherlands increased from 13 in 2014 to 27 in 2018 (Holdert, M. & Kouwenhoven, A., 2018), mainly due to foreign funding.

Imams and preachers play a key role in guiding and encouraging Muslims to live according to Islamic precepts. Promoters of Salafism are conscious of the influence their religious leaders are capable of exerting, especially amongst young people. Therefore, another way of contributing to the spread of Salafism is financing preachers' education and training. Salafist preachers are usually subsidised by countries such as Saudi Arabia in an undercover manner (General Intelligence and Security Service, 2005).

Islamic education outside the Dutch educational system is another powerful tool used to radicalise children and young people. Although it is difficult to conduct radicalisation activities within state-funded schools given the inspection of instructional content and teachers' backgrounds, Salafists have developed other initiatives outside the formal education system. One of them is afterschool classes about Islam and Islamic culture, which can be how Salafists inoculate intolerant and antidemocratic feelings and thoughts amongst young people (General Intelligence and Security Service, 2019).

The last, and probably most effective, tools used to spread Salafist ideology are communication strategies. According to the Dutch General Intelligence and Security Service (2015, p. 7), 'the movement is professional in its communication activities: a large proportion of the information about Islam available to the Dutch public, especially online, reflects a Salafist world view. This helps to explain the popularity of Salafi ideas amongst young Dutch Muslims and converts, in particular'. Promoters of Salafism have developed a coherent communication strategy where a wide range of media outlets are used to reach concrete audiences. They create narratives aimed at presenting themselves as victims of Western societies, and thus trying to exacerbate hostile feelings towards Western values amongst their followers (NATO StratCom CoE, 2019).

Social networks have opened up great opportunities to spread Salafist views amongst Dutch Muslims and potential converts. Before social networks, communication was one-way, from Salafist leaders to followers. After the advent of social networks, communication has become much more horizontal, fast, decentralised and fluid, where any follower can become a loudspeaker for Salafi ideas (Bertholee, R., 2014).

The Dark Web[27] has also been used for Salafist radicalisation purposes in the Netherlands. Radical Salafists often begin to interact through public Internet forums and social media platforms. However, as the radicalisation process progresses, Salafists shift to more extremist forums on the Dark Web (Counter Extremism Project, 2019).

Other traditional components of hybrid threats related to digital technologies, such as cyberattacks, are less common. Radical Salafists have neither the resources nor advanced capabilities to develop harmful cyberattacks, meaning so far action has been limited to a few denial-of-service attacks with propagandistic purposes (Counter Extremism Project, 2019).

4.1.3. Strategy, tactics and tools to counter the hybrid threat

The Dutch authorities' efforts have been focused on countering jihadism, the most extreme level of Salafist radicalisation. In 2014, the National Coordinator for Security and Counterterrorism and the Ministry of Social Affairs and Employment launched the Netherlands Comprehensive Action Programme to Combat Jihadism. It encompassed 38 measures aimed at tackling the jihadist threat in

[27] The Dark Web is a specific part of the Deep Web. The latter refers to internet content that is not indexed by conventional search engines. The Dark Web is a layer within the Deep Web, and it is made up of diverse darknets (TOR, I2P, etc.) that can only be accessed through specific software and browsers which preserve the anonymity of users through encryption systems. Darknets are usually used for malicious or illegal purposes: child pornography, arms and drug traffic, cyber-delinquency, terrorism, etc.

Dutch territory (Inspectorate for Security and Justice, 2017). The measures were classified into five types (Government of the Netherlands, 2014):

- Risk reduction regarding jihadist travellers to conflict zones
- Travel interventions
- Combating radicalisation
- Social media
- Information-sharing and cooperation

While some measures can be considered as being within the realm of traditional counterterrorism (limiting the mobility of alleged jihadists, intensifying prosecution of recruiters for armed struggle, prosecution of hate speech on social networks, etc.) others are aimed at countering the threat of radicalisation in the medium and long term by relying on communication strategies, using both offline and online mechanisms.

One of the measures related to strategic communications to detect and prevent radicalisation is the reinforcement of the communication channels between Dutch authorities and Muslim communities. Engaging moderate imams and mosque administrators to present alternative counter-narratives and increase transparency on Islamic education is an essential instrument to prevent young people of being fascinated by extremist Islamic ideologies. The family and the educational communities were also deemed key actors in preventing radicalisation, and were provided with specific communication tools to help them countering radical ideas:

- Development of networks and online communities to stimulate social integration of young people.
- Inclusion of information about radicalisation on the websites of educational institutions.
- Appointment of a national radicalisation contact point, responsible for investigating reports about alleged jihadist radicalisation.

The commissioning of a channel (a citizens' hotline) to report jihadist content was a prominent measure to combat dissemination of jihadist propaganda through social networks. Although this measure may now seem an obvious response, in 2014 mechanisms for reporting questionable content on social networks were not as usual as they are today. Dutch authorities also proposed the creation of a specialised team within the National Police to detect jihadist content and prosecute its dissemination. Proposals also aimed to engage internet companies to remove jihadist content.

In addition to the measures defined by the Dutch authorities in their action programme to combat jihadism, other stakeholders, from educational institutions to civil society organisations, have also implemented interesting instruments to detect and prevent all kinds of radicalisation, including Salafism. Some examples are showed below:

- The School and Safety Foundation defined a programme to improve the competency of teachers in managing radicalisation in schools. Between 2015 and 2019, more than 3 700 educators were trained to detect and respond to radicalisation in the classrooms (Radicalisation Awareness Network, 2019, p. 110).
- *Echoes of IS*[28] is a web documentary created by Submarine Channel, a production studio focused on new ways of storytelling, with short films about the testimonies of people affected

[28] http://www.echoesofis.nl

by ISIS. The stories are aimed at counteracting the ISIS propaganda targeting young people (Radicalisation Awareness Network, 2019, p. 583).

The strategies implemented by both the Dutch authorities and civil organisations try to address the phenomenon of Salafist radicalisation, as well as other types of radicalisation, in a comprehensive way, including detection, prevention and response actions. In the field of strategic communications, such actions have been focused on debunking jihadist propaganda amongst the most influenceable targets: young people.

4.1.4. Impact and consequences

The impact of Salafist radicalisation in the Netherlands can be noticed when comparing Muslim migrants' feeling of attachment to their host country in the EU. The Netherlands is listed as one of the EU countries where Muslims feel lowest attachment to the country (3.4 points on 5-point scale), along with Italy (3.3 points), Austria (3.5 points) and Greece (3.6 points) (European Union Agency for Fundamental Rights, 2017). As one of the goals of the Salafist movement is to create a society ruled by Sharia law, opposed to Western democracy and values (exemplified by the Netherlands and its social norms), this indicator could show that, to a greater or lesser extent, the Salafist message may receive relative acceptance amongst the Muslim community in the Netherlands, leading to a potentially dangerous rejection of the traditional core values of Dutch society.

It is also interesting to note that the Netherlands and France are the only EU countries where the level of attachment to the country among second-generation migrants is lower than among first-generation ones (European Union Agency for Fundamental Rights, 2017), suggesting that the social disengagement strategies designed by promoters of Salafism and spread through digital means (the means most preferred by young generations) could be succeeding in both countries. However, other factors such as growing islamophobia, promoted by far-right movements and political parties (Damhuis, K., 2019), might be also fuelling Dutch Muslims' lack of attachment to their country.

4.1.5. Conclusions of the case

This case study, in addition to encompassing multiple traditional characteristics of hybrid threats, also presents especial connotations that make it very interesting for the aim of this study. Promoters of Salafism in the Netherlands have used traditional means within the scope of hybrid threats to achieve their goals: foreign support in the form of funding for Salafist organisations and the construction of mosques and Islamic centres, foreign influence through imams and mosque administrators subsidised and trained by the Gulf states, online platforms and digital media outlets to spread their messages and radicalise their supporters, etc. Nevertheless, the major questions that must be asked in order to consider this case study a true hybrid threat are: what are the main goals of promoter of Salafism (both domestic promoters and the foreign countries that support them)? Do the Gulf monarchies want to spread a religious belief or a political and social system that is incompatible with democracy? If the response is that they only seek to promote a religious belief and encourage people to live in accordance with its precepts, there would be no issue and the case could not be considered as a hybrid threat at all. In fact, all religions do the same. However, if the response is that Salafist promoters seek to substitute the liberal democracy established in the Netherlands with new laws and social rules emanating from Salafist doctrine,[29] this is a clear case of a serious threat that uses hybrid methods to succeed.

Dutch authorities and civil society have adopted a cautious approach, facing the potential consequences of the second possibility. Therefore, they have deployed diverse measures to counter the threat that spreading radical Salafism represents for democratic values and social cohesion in the

[29] It is worth noting that Salafism goes beyond religious beliefs, as it also implies a political vision and societal organisation based on the Sharia (Islamic law).

Netherlands. The wide range of actions implemented includes measures at the three stages defined in Chapter 2.2 (preventive, detection and response measures). While response measures are mostly related to punishment and subsequent social reintegration of Salafism supporters once they have been radicalised and have committed illegal actions, preventive measures include all educational initiatives aimed at avoiding radicalisation from infancy. Detection measures are focused on monitoring online and offline activity of potential suspects, as well as Salafist forums and websites, to detect signs of radicalisation.

It can be argued that the Dutch authorities have deployed a coherent communication strategy to counter radicalisation in the information sphere, as the actions follow a systematic long-term plan, involve all stakeholders (families, educational institutions, Islamic centres, imams, etc.), adopt a proactive approach, use adequate channels and narratives, and try to convince the targets (mainly young people) of the alternatives to radical doctrines.

4.2. Case 2: Saudi Arabian pressure on Pakistan in the context of the civil war in Yemen

In the context of the civil war in Yemen, diverse regional powers like Saudi Arabia and Iran have struggled to consolidate their influence. Although the Yemeni conflict has had an eminently local character, it has been used as excuse by Saudi Arabia to exert new ways of influencing other Islamic countries in order to reinforce its leading role in the region.

This case presents an example of a hybrid threat where a regional economic power (Saudi Arabia) tried to influence, by means of economic and diplomatic pressure, the political decision-making process of another country (Pakistan) by taking advantage of its economic weakness.

4.2.1. Geopolitical context

The Yemeni civil war, which is still ongoing, began in early 2015 after the takeover of the capital, Sana'a, by one of the contenders, the Houthi militia. This group, belonging to the Zaidi branch of the Shia confession, emerged in the 2000s as a response to the increasingly authoritative behaviour of the former Yemeni president, Ali Abdullah Saleh, who was deposed in 2011 after the Arab Spring protests. The Houthi militia takes its name from its first leader, Hussein Badreddin al-Houthi, who was a religious leader opposed to the Saleh regime. He was killed by Yemen Army forces in 2004 after being accused by Saleh of creating an armed group called Ansar Allah (Laub, Z. & Robinson, K., 2020).

The Houthi militia, along with other small northern groups and Saleh's supporters who became Houthis allies again after Saleh was overthrown, has been fighting for the control of Yemen since 2015. Its opponents are forces loyal to Saleh's successor, Abd Rabbu Mansour Hadi, who controls the South and West of Yemen. While the Houthi militia has been supported by the Iranian regime, mainly through the provision of weapons, Hadi's forces are backed by a coalition of Sunni-majority Arab states, led by Saudi Arabia (Laub, Z. & Robinson, K., 2020). There are also other factions involved in this conflict, such as Al-Qaeda in the Arabian Peninsula (AQAP). AQAP, which has been responsible for some terrorist attacks in Western countries,[30] controls a small territory in central Yemen. Another group is the separatist Southern Transitional Council (STC). In 2019, this faction was backed by the United Arab Emirates (UAE), whose objective is to increase its influence in the South and, especially in the strategic ports along the coast of southern Yemen, which constitute key infrastructure for UAE interests (Lackner, H., 2020). The STC and president Hadi reached an agreement in late 2019 to share power in a Yemeni post-war government and concentrate their efforts on defeating Houthi forces in the North and AQAP in the centre of Yemen.

[30] Charlie Hebdo shooting in Paris in 2015; Shooting in a classroom building at the Naval Air Station at Pensacola (USA) in December 2019

Soon after Sana'a was taken over by the Houthis, Saudi Arabia, where president Hadi was exiled, launched a joint armed operation, called *Operation Decisive Storm*, for which it sought material and logistical support from other Arab countries. The Saudi-led coalition that aimed to defeat the Houthis and restore Hadi as Yemeni president, was initially made up of Bahrain, Egypt, Jordan, Kuwait, Morocco, Qatar, Sudan and the United Arab Emirates (Laub, Z. & Robinson, K., 2020). Surprisingly, one of the Saudi Arabia's closest allies, Pakistan, refused to join the coalition. The Pakistani Parliament voted to remain neutral in the conflict (NATO StratCom CoE, 2019). It was not until 2018 that Pakistan decided to join the coalition, but only by sending troops to Saudi Arabia in advisory and training roles.

Saudi Arabia exerted its economic and diplomatic influence to convince Pakistan to join the coalition. Its resistance was derived from the intention of not interfering with its neighbour, Iran, by meddling in its interests (Iran was allegedly supporting the Houthi armed group) (NATO StratCom CoE, 2019). In particular, Pakistan did not want to put its diplomatic relationships with Iran at risk just when Western sanctions on Iran, motivated by the Iranian nuclear programmes, seemed close to being lifted and Pakistan could again expect to purchase fossil fuels from its neighbour (NATO StratCom CoE, 2019).

4.2.2. Features of the hybrid threat

Saudi Arabia was eager to get Pakistan involved in the armed coalition to increase its chances of success in the Yemeni war. As a result of its longstanding latent conflict with India and the need to deal with many domestic conflicts (religious tension between diverse Muslim confessions, extremist terrorism, etc.), Pakistan has one of the strongest armies in the world. According to Global Firepower, an online publication that assesses the strength of 138 military powers every year, in the last fifteen years the Pakistani army has always ranked amongst the top 20 most powerful armies in the world (GlobalFirePower, 2020). Of Muslim majority countries, Pakistan has always been in the top 4, along with Egypt, Turkey and Iran. Therefore, it is not surprising that Saudi Arabia sought Pakistan's participation in its coalition. Saudi Arabia combined economic and diplomatic pressures, as well as religious affairs, to achieve its aim.

Saudi Arabia has become one of the biggest financial supporters of Pakistan, along with the US and China. For instance, in early 2019, Saudi Arabia offered Pakistan an investment deal worth US$20 billion (BBC, 2019). In 2018, Saudi Arabia granted financial support worth US$6 billion to help Pakistan avoid a balance of payments crisis (Bokhari, F. et al., 2018). In late 2014, before the Yemeni civil war started, Pakistan received US$3 billion from Saudi Arabia to stabilise the rupee's value against the US dollar. Shortly afterwards, Pakistan confirmed its support for the Saudi position on the Syrian conflict (BBC, 2015). This last example shows how Saudi Arabia has traditionally used financial support to achieve its strategic goals, in this case trying to engage Pakistan, the only Muslim majority country that is a nuclear power, in the anti-Houthi coalition.

Another element of economic pressure that Saudi Arabia could have used to influence Pakistan is the great number of Pakistani workers in Saudi territory. According to the Ministry of Overseas Pakistanis & Human Resources Development of Pakistan (2019), in December 2017 there were 2.6 million Pakistanis living, working or studying in Saudi Arabia. Between 2013 and 2018, Pakistani workers sent remittances to Pakistan worth more than US$26.6 billion (about US$5 billion per year), a crucial source of income for the Pakistani economy. Any decision that reduced the number of Pakistanis working in Saudi Arabia and replaced them with workers from other countries could cause serious damage to Pakistan's economy. There is no evidence that Saudi Arabia exerted this kind of economic pressure to convince Pakistan to join the anti-Houthi coalition; however, it is a plausible scenario. Recent information highlighted the fact that Saudi Arabia could have used this threat to impede Pakistan attending the Kuala Lumpur Summit, a global platform for dialogue amongst Muslim countries that Saudi Arabia tried to boycott (Altay, I., 2019). Saudi Arabia dismissed the accusations of pressure on Pakistan and dubbed the information as false (Siddiqui, N., 2019).

Religious matters have also been used by Saudi Arabia to influence Pakistan. Although religious influence is not limited to the specific case of Pakistani participation in the Operation Decisive Storm,

it is interesting to analyse how Saudi Arabia has tried to expand Wahhabism throughout the Islamic world to counter any pro-Iranian Shia expansion from its main rival in the Middle East (Afzal, M., 2019). Since the 1970s, Saudi Arabia has been allegedly financing madrassas (Islamic schools) in Pakistan to promote its conservative version of Sunni-Islam with a double objective: replace the traditional Sufi Islam practised in many Pakistani regions and curb the Iranian expansion (Afzal, M., 2019). The result of this radicalisation is an increase in attacks on religious minorities, including Shia populations (Yousaf, F., 2016).

4.2.3. Strategy, tactics and tools to counter the hybrid threat

Pakistan deployed diverse strategies, ranging from diplomatic to economic tools, to counter Saudi attempts to influence its decisions regarding participation in the Yemeni civil war. In the field of diplomacy, Pakistan tried to remain neutral between the two regional powers, Saudi Arabia and Iran, for whom the Yemeni civil war was merely another stage of their ongoing rivalry. As Pakistan's economy depended on both continued Saudi financial support and access to Iranian crude oil, Pakistan sought to remain neutral. The Pakistani Parliament passed a resolution refusing to help Saudi Arabia with armed troops, stating that 'Pakistan should maintain neutrality in the Yemen conflict so as to be able to play a proactive diplomatic role to end the crisis' (Mahmood, F. & Ali, A., 2015). However, the resolution also highlighted Pakistan's firm commitment to Saudi Arabia and expressed 'unequivocal support for the Kingdom of Saudi Arabia', and affirmed that 'in case of violation of its territorial integrity or any threat to Islamic holy places, Pakistan will stand shoulder to shoulder with Saudi Arabia and its people' (Mahmood, F. & Ali, A., 2015). Although the Pakistani Parliament initially refused supporting Saudi Arabia, the Pakistani narrative left the option of future interventions open, so as not to upset the Saudis too much.

In the economic sphere, Pakistan counted on another relevant ally: China (NATO StratCom CoE, 2019). The Chinese government was very interested in ensuring peace and stability in the Middle East in order to facilitate the development of large infrastructure projects linked to its *Belt and Road Initiative*[31]. For that reason, China backed Pakistan's decision to remain neutral in the Yemeni conflict, and was willing to financially support Pakistan just in case its decision caused the withdrawal of Saudi funding (NATO StratCom CoE, 2019). Therefore, Pakistan was able to risk facing a strategic economic partner, Saudi Arabia, as its decision allowed it to strengthen the economic ties with another, China.

4.2.4. Impact and consequences

The immediate consequence of Pakistan's refusal to collaborate in Operation Decisive Storm was the warning threats launched by one of the participants in the anti-Houthi coalition, the United Arab Emirates, whose Ministry of State for Foreign Affairs declared, shortly after the approval of the Pakistani parliament resolution, that Pakistan would pay a heavy price for its ambiguous stand on the Yemeni conflict (Dawn.com, 2015). Although the Saudis did not comment on the rejection of its collaboration request, the statement of the UAE Ministry was deemed as the official position of the coalition and its leader, Saudi Arabia. Pakistan, given the great pressure exerted by some members of the anti-Houthi coalition, had to send a delegation to Saudi Arabia to explain the terms of its resolution, claiming that a nuclear power like Pakistan should act as responsible mediator (Shiraz, C., 2015).

Three years after it declined to participate in the coalition, Pakistan agreed to send troops to Saudi Arabia on a training and advisory mission (Panda, A., 2018). This strategic movement could be seen as a contradiction of the initial resolution. However, Pakistan's narrative explaining its change of mind continued to focus on the idea of neutrality. The statement issued by the Pakistani army declared that 'the contingent already there [Saudi Arabia] will not be employed outside the Kingdom of Saudi Arabia',

[31] The Belt and Road Initiative was launched in 2013 by the Chinese leader Xi Jinping to develop infrastructures (railways, highways, power grids, etc.) to facilitate the flow of goods, persons and capital between China, the rest of Asia, Europe and Africa in order to expand China's influence in the world (Chatzky, A. & McBride J., 2020).

highlighting that Pakistani troops would not enter combat on Yemeni soil (Panda, A., 2018). Although Pakistan finally bowed to Saudi Arabian demands (three years after the Yemeni civil war started and only in a secondary role) its communication strategy was coherent over time, allowing its two main objectives to be met: to present Pakistan as a neutral country in the Yemeni conflict to the international community (and mainly to key stakeholders like Iran and China), and to continue being considered a major and reliable partner by Saudi Arabia.

From the Pakistani perspective, its initial neutral position, upheld under the pressure of Saudi Arabia and its allies in Operation Decisive Storm, opened up the possibility of tightening economic ties with China, thus reducing its financial dependence on Western countries and Gulf monarchies.

4.2.5. Conclusions of the case

This case study analyses diverse ways of influencing sovereign decisions of a foreign country in a complex geopolitical scenario. The hybrid threat was based on economic and diplomatic pressure. Religious influence, although not explicitly designed for this specific hybrid threat, was also used.

The intervention of Saudi Arabia, trying to incorporate Pakistan in the armed coalition against the Houthi militia in the Yemeni civil war, presents some of the essential characteristics of hybrid threats:

- It was aimed at favouring the strategic goals of Saudi Arabia: to defeat the Houthi militia in Yemen and become the leading partner in the reconstruction of the country.
- It targeted Pakistan's systemic vulnerabilities: its economic weakness and foreign financial dependence.
- It was intended to influence the decision-making processes of Pakistani authorities regarding the country's level of involvement in the Yemeni civil war.

Pakistan adopted a successful communication strategy to counter the pressure exerted by Saudi Arabia and other members of the anti-Houthi coalition. It was focused on proclaiming the neutrality of Pakistan in the Yemeni conflict. The Pakistani Parliament's own resolution based the rejection of the Saudi request on the Pakistan's desire to remain neutral. Although Pakistan finally supported the armed coalition (three years after its creation and only providing advisory and training support to the Saudi army on its own soil), it kept stressing its neutral role in the conflict. This way, Pakistan was able to preserve its longstanding and friendly relationship with its closest strategic partner, Saudi Arabia, and contribute to the regional interests of its two other key partners, Iran and China, with its neutral position.

4.3. Case 3: Foreign influence of Russia and China through academic institutions and think tanks

As explained in Chapter 2.1, soft power is an important means of influence. When properly combined with hard power, it can constitute a hybrid threat. A clear example of the use of soft power tools as part of a hybrid threat is the influence exerted by foreign countries through government-funded organisations. Countries create and finance different types of organisations that are similar in nature (think tanks, NGOs, academic institutions) to spread a positive image of themselves, influence national or regional policy-making, as well as to promote their views on a wide range of political and social issues.

This case study addresses two examples of this strategy. The first is the Chinese *Confucius Institute* (CI). In recent years, China has adopted new soft power strategies in line with its renewed and more proactive foreign policy. CIs are language teaching institutions which have experienced great proliferation around the world. The other case is the Russian think tank *Institute of Democracy and Cooperation* (IDC). In contrast with China, Russia already has significant experience in foreign

influencing strategies through soft power mechanisms. The IDC is one of the numerous institutions funded by Russia to promote its desired international image.

4.3.1. Geopolitical context

Since the middle 2000s, the People's Republic of China has been gradually shifting its role in the international scene. Under the current leadership of the President Xi Jinping, and based on its economic strength, China is evolving from the low international profile maintained during the second half of the last century towards a more relevant presence in global relations (Esteban, M., 2016). The foreign policy of Xi Jinping, modelled on his predecessor's *theory of peaceful rise* (Brookings, 2005), is based on the need for cooperation to face global challenges. In this sense, the image of China abroad becomes especially relevant (Esteban, M., 2017). For that reason, China's foreign policymakers have designed new strategies based on soft power tools.

Propaganda has been used by the communist regime since the 1930s (Starr, D., 2009). However, a new soft power policy was designed under the presidency of Hu Jintao (Xi Jinping's predecessor). In 2006, the former President of Xi'an International University, Du Ruiqing, gave some clues about China's new attitude towards its soft power strategy: 'It is time to make ourselves better understood by the world's people […] Once they come to know the Chinese people better, they will find out that harmony is an essential part of Chinese tradition and a country that values harmony poses absolutely no threat to the rest of the world […] Culture is a soft power that effectively penetrates to quench misunderstanding and hostility between people of different races […] China should help people from other nations acquaint themselves with Chinese culture, including traditions, religions and particularly the Chinese way of thinking. This will help China overcome its cultural deficit' (China Daily, 2006).

At the 17th National Congress of the Communist Party of China, Hu Jintao recognised the importance of Chinese culture as part of its development and growth: 'The great rejuvenation of the Chinese nation will definitely be accompanied by the thriving of Chinese culture' (Jintao, H., 2007). Current president Xi Jinping was more explicit some years later: 'We should increase China's soft power, give a good Chinese narrative, and better communicate China's message to the world' (Biswas, A. & Tortajada, C., 2018).

Russia has always understood conflict as a continuum. Since the times of Soviet Union, Moscow's long-term objective has been to shape opinions and public debate towards Russia's own interests and 'deposit an ideological base that eases the path for subsequent influence operations' (EPRS, 2018). In order to restore *Russian greatness*, Russia is making use of the old Soviet influence toolbox, and has renewed it in recent years with some measures such as cyberwar techniques. This toolbox includes active measures, disinformation campaigns, agents of influence, reflexive control, forgeries, propaganda and controlled international front groups (EPRS, 2018).

After the first negative experiences regarding the Colour Revolutions,[32] Russia became aware of the importance of ideas and legitimacy. A favourable public opinion and/or a foreign elite without legitimacy could be more effective than many weapons. In this sense, Russia decided to add a new instrument to its influence toolbox, one based on a soft power: NGOs and Think Tanks to spread Russia's vision around the world. (Popescu, N., 2006). Russia's intention was: 'To develop an efficient infrastructure of ideas, institutions, networks and media outlets that can use the predictable crisis of the current Orange-type regimes to regain influence not simply at the level of government but at the level of society as well' (Krastev, I., 2005). Russia developed its NGO infrastructure and its channels to spread the Kremlin's message everywhere (Popescu, N., 2006).

[32] The 'Colour Revolutions' is the name given to a group of democratisation processes in the 1990s and 2000s which led to the overthrow of authoritarian governments in the countries where they took place. Depending on the author, the list of Colour Revolutions includes Serbia, Georgia, Ukraine, Romania, Slovakia and Kyrgyzstan. These processes were characterised as being peaceful, and were carried out in former Soviet countries. (Stewart, 2009).

Europe is the main objective of Russian pressure in its return to greatness. From the conflict in Ukraine and Crimea to the Brexit process, passing through the Baltic region, many countries in Europe have suffered or are suffering the effects of the Russian soft power. (NATO StratCom CoE, 2019).

4.3.2. Features of the hybrid threat

The Confucius Institutes

The First CI was established in Seoul, South Korea, in 2004. In 2017, the number of CIs in the world was 525, most of them distributed between Europe, America and, to some extent, Asia (NATO StratCom Centre of Excellence, 2018).

According to the constitution and by-laws of the Confucius Institute, its main function is teaching the Chinese language (Mandarin) in foreign countries. The objectives are not only to satisfy the demand of people wanting to learn Chinese in different countries around the world but also to improve educational and cultural cooperation between China and other nations. Another relevant goal is 'deepening friendly relationships with other nations, to promote the development of multi-culturalism, and to construct a harmonious world' (Confucius Institute, n.d.). Management of the CI is centralised in headquarters (known as Hanban), which are located in China and depends on the Ministry of Education.

The CI is flexible in its configuration, which facilitates its proliferation. Any educational entity interested in teaching Mandarin must meet only a few lax requirements before asking the headquarters for permission to establish a CI branch. The new branch would then be co-directed by a member from the host country and a Hanban officer.

Despite its benevolent and generally acceptable purposes, point six of its General Principles (constitution and by-laws) has created mistrust in foreign stakeholders interested in the establishment of CI branches. It states that the Institute should respect the law, the cultural and educational traditions and social customs of the host country. However, it also adds that the Institutes cannot contravene Chinese laws. Other points of the CI statutes also make it clear that Chinese representatives in each branch are under the strict control of Hanban headquarters. (Confucius Institute, n.d.).

In practice, there have been some incidents related to the aforementioned clause that have concluded in the non-renewal of several CI contracts. In 2013, McMaster University in Hamilton (Canada) ended its contract with the Confucius Institute due to a legal issue with a former Chinese teacher, Sonia Zhao, who made a complaint against the university to the Ontario Human Rights Tribunal because she was obligated by contract to hide her creed, Falun Gong (a Chinese spiritual practise). Hanban hired the teachers from China and therefore imposed this obligation (Bradshaw, J. & Freeze, C., 2013). Another case took place during the European Association for Chinese Studies Conference in Braga (Portugal). Xu Lin, at that time the Director-General of the Confucius Institute Headquarters, ordered some pages of the Conference Programme to be cut. Those pages contained information related to the Chiang Ching-Kuo Foundation, another academic institution focused on promoting Chinese culture around the world, which is located in Taiwan, a Chinese region in permanent conflict with Beijing regarding its political status. (EACS, 2014).

After the McMaster case, many other cases of CI branches meddling in order to influence activities, events, or production of the host academic institutions have been reported. (Sahlins, M., 2014). As a consequence, there is a growing common opinion of rejection towards the Confucius Institute in the academic sphere.

In 2014, the Canadian Association of University Teachers called all universities to end relations with the Institute (CAUT, 2014). Months later, the American Association of University Professors did the same. (AAUP, 2014). In 2017, the American National Association of Scholars released an extensive report about the Confucius Institute, arguing why all universities should terminate their relations with the Chinese institution (Petterson, R., 2017).

In Europe there have also been reactions to the potential risks of CI interference. In November 2019, the Foreign Affairs Committee of the House of Commons drew attention to 'autocracies' influence on academic freedom in the UK', and recommended further risk assessment, strengthening collaborations and implementing a sanctions policy (House of Commons. Foreign Affairs Committee, 2019). Universities in Sweden and the Netherlands have closed CIs in recent years (Bentzen, N., 2019). The Vrije Universiteit Brussel announced in December 2019 that it will not extend its contract with the CI, which expired in June 2020, and stated that 'The VUB is always open to new collaborations with Chinese universities, scientists and students, on the condition that academic freedom and independence can be guaranteed in mutual trust' (Vrije Universiteit Brussel, 2019).

Finally, a report from the USA's Senate stated that 'CI's funding comes with strings that can compromise academic freedom' (Portman, R. & Carper, T., 2019). The report argued that: (1) USA's educational institutions were accepting by contract China's legislation by contract; (2) China was trying to export its censorship; (3) China wanted to change its image as an economic and security threat in Western countries. This report suggested that the Confucius Institute may constitute a hybrid threat in the form of a soft power tool.

Russian think tanks and NGOs

There are numerous and varied soft power organisations related to the Russian administration. These organisations are characterised by three elements. First, location; they can be established in Russian territory or abroad. Second, the nature of their economic relationship with the Russian Government and the level of transparency of their funding, as the Kremlin sometimes prefers not to be directly linked to these NGOs and think tanks. And third, their goals:

- Many organisations are created to support what Russia calls compatriots abroad. Compatriots are citizens of other countries (mainly former Soviet countries) with Russian roots, or who belong to Russian speaking communities. These people are considered part of the country even though they live abroad and the Government tries to keep their Russian identity and feelings alive through these organisations. Functionally, these institutions are governmental-organised non-governmental organisations (GONGOs). They receive funds from the Russian government, normally via the Ministry of Foreign Affairs. There is a World Coordination Council of Russian Compatriots to coordinate all these GONGOs. They include *Russkiy Mir* and the *Foundation for Supporting and Protecting the Rights of Compatriots Living Abroad*. (Vojtíškova, V. et al., 2016).
- Other Russian organisations abroad are dedicated to the production and dissemination of Russian ideas and views, and to the promotion of a positive image of the country. Their aim is to present an alternative to Western culture and liberal democracy. These organisations are usually established as NGOs (undercover GONGOs) or think tanks. Their funding remains rather opaque in their accountability. While some of them receive government financial support, which sometimes is hidden through intermediaries, other institutions are funded by private donations. For example, the *Alexander Gorchakov Public Diplomacy Fund* is financially supported by the Ministry of Foreign Affairs. However, the only available information about funding of the think tank *Dialogue of Civilisations* is the existence of a foundation with a similar name in Switzerland (Vendil, C. & Oxenstierna, S., 2017).

Russia has deployed several GONGOs and/or think tanks in European territory: *Dialogue of Civilisation Research Institute* (Berlin, 2016), and the *Institute of Democracy and Cooperation* (Paris, 2008), amongst others. These institutions have the task of promoting the Russia's political vision as an alternative to Western liberal democracies' narrative, as well as improving the image of Russia abroad. To accomplish their mission, they produce knowledge in the form of studies and academic papers and organise activities such as conferences and events. This modus operandi could be dubbed as an intellectual lobbying (Vojtíškova, V. et al., 2016). Let us look at a concrete example.

The Institute of Democracy and Cooperation (IDC) is a think tank established in Paris in 2008. In 2015 the IDC received consultative status from the Economic and Social Council of the United Nations (Institute of Democracy and Cooperation, 2016). The Institute can be considered as a GONGO. According to *Wikileaks*[33], its foundation was the responsibility of the Government of Russia. Natalia Narochnitskaya is the current Director. She is a Russian politician, historian and diplomat. She was an elected representative at the Russian State Duma between 2003 and 2007, and served as vice chair of the International Affairs Committee in the State Duma. The second in charge of the IDC is the director of studies, John Laughland, a British Doctor of Philosophy specialising in international affairs. Before working for the IDC, he directed the Eurosceptic think tank European Foundation[34] (Vendil, C. & Oxenstierna, S., 2017). According to its website, the IDC organises conferences and discussions on contemporary matters of interest: the role of history in contemporary politics, East-West relations, sovereignty and human rights, etc. (Institute of Democracy and Cooperation, 2016). The IDC intends to provide another approach to human rights as an alternative to the Western one, as well as to present Russia's vision of the main historical events of the last two centuries.

4.3.3. Strategy, tactics and tools to counter the hybrid threat

In its report on the Confucius Institute, NATO's Strategic Communication Centre of Excellence gave three recommendations to counter its influence (NATO StratCom Centre of Excellence, 2018):

- Raise awareness about the real status of Confucius Institutes. These institutions should be considered centres to promote Chinese language and culture, but not providers of expertise in other topics. Given its strong dependence on the Chinese Administration, objectivity regarding sensitive topics must not be expected.
- Reform the funding of CIs to achieve greater autonomy and financial independence for the branches, whose funding strongly depended on China's headquarter budget.
- Audits should be periodically conducted to ensure academic freedom and the absence of censorship. Chinese studies programmes at the host institution should be completely separate from CIs.

The National Association of Scholars report mentioned above, proposed recommendations to restrict Chinese power over CI branches and ensure academic freedom. It also advised the US Congress to investigate whether American interests could be threatened by the Confucius Institute. The most energic recommendation was, however, to close all CI branches in the USA. (Petterson, R., 2017).

The Senate staff report *China's Impact on the U.S. Education System* also provided a set of recommendations to several institutions. Most of them were related to the transparency and control of CI branches. One of the recommendations urged the Justice Department to investigate whether the Confucius Institute intended to influence the Government or public opinion, in order to register it under the Foreign Agents Registration Act (Portman, R. & Carper, T., 2019).

In Australia, the Government announced a University Foreign Interference Taskforce to guarantee academic freedom. In November 2019, it published *Guidelines to counter foreign interference in the Australian university sector,* providing recommendations to safeguard a balance between the openness of the university system and its quality and freedom (University Foreign Interference Taskforce, 2019).

[33] The Institute for Democracy and Cooperation: Russia's new face to the world: https://wikileaks.org/plusd/cables/08MOSCOW375_a.html. Also referred to in (Vojtíškova, V. et al., 2016) and (Vendil, C. & Oxenstierna, S., 2017).

[34] https://europeanfoundation.org/about/

The European Parliament has called for actions to guarantee the autonomy of education institutions, as a precondition for academic freedom, in the 2018 resolution *Defence of academic freedom in the EU's external action* (European Parliament, 2018b).

Whatever strategy to counter the threat that NGOs and think tanks could represent to the sovereignty of foreign countries should be based on respect for freedom of expression and association. This starting point implies further difficulties in dealing with these hybrid threats when compared to other types. Regarding pro-Russian think tanks, the NATO StratCom CoE suggested improving collaboration between nations to investigate the relations around these organisations. It also proposed raising awareness of their real aim and unclear links. The last NATO recommendation was to 'increase the level of accountability and financial transparency' (NATO StratCom CoE, 2019), which would help to expose the real objective of Russian think tanks and NGOs.

4.3.4. Impact and consequences

According to the NATO StratCom CoE report, in terms of informational impacts, the Confucius Institute was a successful policy, given the great growth of China's presence in the USA. Even outside cities, where there were fewer opportunities to expand Chinese learning, CI branches were proliferating. As every CI centre was a hotspot for the transmission of China's message, the fact that so many branches were opened could be considered a success (NATO StratCom Centre of Excellence, 2018).

One potential consequence of CI proliferation was its influence on public opinion, which in turn could affect decision-making processes. Following this logic, it may affect or alter (NATO StratCom Centre of Excellence, 2018):

- the sovereignty of foreign policy and internal mechanisms of foreign policy decision-making;
- the integrity and consistency of internal public opinion of external actors (other countries);
- the integrity and consistency of academic research about China.

In the academic sphere, it was also possible to find some vulnerabilities revealed by the CIs' activity. The collaboration between the CI and the host academic organisation involved sharing critical infrastructure (digital academic networks) which, in turn, could allow China access to crucial data. Another vulnerability was the limited budget that host academic institutions normally possessed. The financial resources that usually accompanied the establishment of Confucius Institutes was a good incentive for the host institution to give way to Chinese influence. (NATO StratCom Centre of Excellence, 2018). As a result, the collaboration with the CI could represent a threat to the future of the academic independence in the host countries.

The common guidelines ruling the CI centres (commanded from Hanban) regarding what to promote or not could directly affect the freedom of academic production in the host country. Since the opening of CI centres consisted of a partnership, the censorship imposed from China could also affect the host institution and its academic cooperation with other partners that opposed to China's policies. (NATO StratCom Centre of Excellence, 2018).

The conflicts between academic freedom and CI action seem to have been more evident in countries with an Anglo-Saxon tradition such as Canada, the United States, Australia and the United Kingdom. Higher education systems in these countries are highly dependent on private funding (OECD, 2019), including tuition fees, grants and private benefactors. Foreign students comprise a great share of tuition fees, particularly in top universities, and Chinese students represent an increasing part of international students. In Australia, Chinese students represent 33% of all foreign enrolments (Maslen, G., 2019) and their fees make up to a fifth of the total annual revenue of the University of Sydney (Robinson, N., 2019). Chinese students contributed US$12 billion to the US higher education system in 2017 (Skinner, M., 2019).

Although there are many differences between EU Member States, within the EU there is generally more of a shared belief that higher educations should be largely financed through public resources (Arnhold, N. et al., 2020). However, globalisation and economic crisis have pushed funding reforms in order to increase diversification of revenues at European universities. Trends include an increase in private funding compared to public funding, and a shift away from direct funding to indirect, competitive, funding (Jongbloed, B., 2018). The shift towards a more market-oriented university may increase its vulnerability to organisations such as the CI, which attract tuition fees from Chinese students, fund scholarships for local students to study in China and offer financial incentives to host academic institutions (Petterson, R., 2017).

Regarding Russian influence, the activity of the IDC in France may have had consequences for the security and stability of the country. Consequences could also be applicable to Europe due to the international diffusion of IDC activities (NATO StratCom CoE, 2019):

1. Some critical functions of French democracy could be affected by the IDC, mainly:
   - public opinion and debate, damaged by using heavily biased and manipulated arguments,
   - trust in government institutions,
   - and the health of civil society and its plurality and progress.
2. Regarding the alleged vulnerabilities of Western democracies exposed by the IDC activity, NATO pointed out the proliferation of anti-American sentiments, as well as the exacerbation of conservative-liberal cleavage due to the conservative character of the IDC on social issues.
3. The strengthening of far-right movements and political polarisation.

Regarding the effects of IDC activities, their limited scope must be taken into account. The organisation's scarce resources and its low presence in mainstream media and social media led to a low impact on society. The IDC's lobbying activity of the IDC may be more effective in decision-making processes. However, in spite of the efforts of the IDC and in line with the low impact of the think tank, French opinion surveys showed that anti-Russian feelings predominated in French society (NATO StratCom CoE, 2019).

Despite China and Russia's efforts to improve their image abroad and influence local policy-making processes, they appear at the bottom of the Soft Power 30 Index[35]. China achieved its best position in 2017 (27th) while Russia occupied the last position of the ranking between 2016 and 2019, except for 2017, when it ranked 29th.

4.3.5. Conclusions of the case

Considered in isolation, cultural and academic influence cannot be strictly seen as a hybrid threat, but it represents yet another hybrid tool, a key component of the threats eroding academic independence and trying to influence public opinion and, as a consequence, public representatives. This kind of tool is an example of how the line between influence and interference in national affairs is blurred by hybrid threats.

The response from academic institutions, where they have occurred, to the risks to academic freedom that these organisations pose to Western democracies has been to terminate relations. Countries such as Australia, Canada and the United States, as well as NATO, have issued recommendations in that vein, in addition to raising awareness about the threat.

The aforementioned *Guidelines to counter foreign interference in the Australian university sector* (University Foreign Interference Taskforce, 2019) include 'Communication and education' as one of the

[35] The Soft Power 30: https://softpower30.com/

four strategic areas, with the objective of raising awareness about foreign interference amongst university staff, students and decision makers, and increasing resilience. The Association of American Universities has also published guidelines and good practices on awareness building and communications to limit foreign interference, as well as strengthening cooperation with federal security and intelligence agencies (American Association of Universities, 2019).

In Europe, the Covid-19 crisis has put extra pressure on academic institutions, which are facing a complex financial situation derived from the drastic reduction of tuition fees (Arnhold, N. et al., 2020). This crisis might increase the risks derived from the economic benefits of agreements with foreign institutions such as the CI and internationalisation, at the expense of academic freedom.

A robust, diversified and sustainable funding system for European Universities, together with appropriate measures to ensure transparency and awareness amongst the academic community and society as a whole, are needed to guarantee their role as drivers of innovation, social cohesion, knowledge generation and critical thinking in our democracy.

4.4. Case 4: Russian intervention in Ukraine

If a paradigmatic case where all the components of hybrid threats were put in place to influence the target had to be selected, it would undoubtedly be the Russian intervention in Ukraine, especially between 2013 and 2015. During that period, Russia developed an intense hybrid campaign in order to impede Ukraine's geopolitical shift towards a tighter collaboration with the European Union. Russia combined economic, diplomatic, military and legal action, as well as cyberattacks and disinformation campaigns, to influence Ukrainian domestic and foreign affairs. As has been stated, 'Ukraine is undoubtedly a very specific case and several specific factors enabled effective hybrid warfare in order to achieve the political end: the annexation of Crimea and therefore the demonstration of great Russia revival' (Rusnáková, S., 2017, p. 353).

In order to justify its intervention, Russia developed a narrative based on both preserving Russian identity in Ukraine and defending Russian minorities.

4.4.1. Geopolitical context

Ukraine is one of the largest countries in Europe. Its geographical situation, between Russia and the European Union, is strategic from an economic perspective, as it is crossed by several gas pipelines through which a large part of the gas sold by Russia to Europe flows.

Prior to the 2014 crisis, Ukraine had moved closer to the EU using the framework of a possible 'Association Agreement' (a cooperation treaty between the EU, its Member States and a non-EU third country), with the aim of eventually joining the Union. Surprisingly, on 21st November 2013, the Ukrainian government, leaded by the President Victor Yanukovych, suspended the process of signing the Association Agreement, which had been intensively negotiated over the past six years, yielding to Russian pressure. The Ukrainian government also decided to resume economic negotiations with CIS Member States (Interfax-Ukraine, 2013). The Kiev government justified itself by saying that the agreement with the European Union would have an excessive cost to its economy, which heavily depended on Russia (The Guardian, 2013). The Ukrainian government's decision gave rise to what was called *Euromaidan*, massive demonstrations in Kiev's Independence Square in which the population showed its disagreement with that decision.

Moscow's strategy was to attract the former Soviet Republics by creating a new economic alliance, the Euroasian Economic Union (just like the EU). To reach this goal, Russia used all elements of the hybrid threats to ensure that Ukraine would not enter into any agreement with the EU, since the former Soviet Republic represented a major source of economic income for Russia that it could not afford to lose. Apart from the fact that the Russian army depended partly on the Ukrainian military and aeronautical industry (Recknagel, C., 2014), it is interesting to note that Russia's income from energy exports

accounted for 22% of its GDP in 2014 (6.7% of GDP came from gas exports) and most of the gas supplied by Russia to European countries was channelled through the Soyuz pipeline, which passes through Ukraine (Álvarez, G., 2014). Both examples of Russian-Ukrainian economic interdependency show the Russian need to keep Ukraine under its political influence.

4.4.2. Features of the hybrid threat

Russia developed an aggressive hybrid campaign against Ukraine by combining diverse components, ranging from economic pressure to digital activities such as cyberattacks. All of them are analysed in this section.

Economic pressure

After the break-up of the USSR, Ukraine, unlike Kazakhstan and Azerbaijan, had hardly any internal reserves to finance any reforms, with its economy being particularly susceptible to external influence (Wilson, A., 2014).

Prior to the 2014 Ukrainian crisis, the Kremlin used the asymmetric relationship of Ukraine's economic dependence on Russia to influence Kiev; first, in the form of highly subsidised oil prices during Kuchma's presidency; second, by punishing the Kiev government through supply disruptions and raising oil prices during Yushchenko's more European-oriented presidency. In practice, Russia has bought the loyalty of the Ukrainian government by subsidising oil and gas prices since the Orange Revolution [36] in 2004 (Newnham, R., 2011).

At the peak of the crisis, many Ukrainian companies, whose only customer was Russia (Russia was by far the largest market for Ukrainian products, with a 25 % share), could only survive with government aid and subsidies, not to mention the loss of a third of their experts, who moved to Russia (Lázaro, A., 2014).

To prevent the agreement being signed between the EU and Ukraine, Russia threatened the Ukrainian economy by adopting a set of measures (Álvarez, G., 2014):

- It suspended the tariff-free import quotas for Ukrainian steel pipes, which made the price on the Russian market 20 % higher.
- It banned the import of *Roshen* brand chocolates, which meant about US$100 million in losses for the Ukrainian firm.
- It changed the credit rating of Ukrainian importers to '*risky*'.
- It restricted the import of meat products from Ukraine.
- It withdrew production licences from Ukrainian railway wagon manufacturers.

When the separatist movements began to take shape in the Donbass area, one of the areas where the armed conflict was more intense, its industrial elite supported such (pro-Russian) actions, since a rapprochement with the EU could infringe further damage to their local industry, given that their exports were mainly directed towards Russia (Zhukov, Y., 2015). They also assumed that maintaining the status quo in the region could only be achieved through closer cooperation with Russia rather than the possible integration with the EU, which would force them to adopt stricter anti-corruption standards (Sommerbauer, J., 2016).

[36] The Orange Revolution is the name given to a series of non-violent demonstrations after the 2004 presidential elections, where supporters of the opposition candidate Viktor Yushchenko protested against alleged electoral fraud, which would have benefited the government-backed candidate Viktor Yanukovych. The elections were re-held in December 2004 and Viktor Yushchenko became the legitimate president of Ukraine.

Military actions

Within the framework of Russian pressure on Ukraine, military actions, overt and covert, were focused on two specific events:

a) The illegal annexation of Crimea by Russia

The refusal to sign the Ukraine-EU Association Agreement gave rise to the Euromaidan protests movement, which, in the end, caused the fall of the Yanukovych's government. In Crimea, the removal of Viktor Yanukovych as Ukrainian president led to a political crisis, in which various pro-Russian groups demonstrated against the new government and proclaimed their desire to strengthen their ties (or even reintegrate) with the Russian Federation. As a result, Crimea witnessed numerous armed and military revolts between pro-Russian and pro-European groups (Bebler, A., 2015). At the end of February 2014, taking advantage of the political instability in Crimea, troops with unmarked uniforms (called 'little green men') occupied strategic positions, cutting off communication between Ukraine and Crimea. After the annexation, Russia eventually acknowledged that these troops belonged to the Russian Special Forces (Schreck, C., 2019).

In March 2014, Crimean local authorities recognised Russian authority over the peninsula. Russia consolidated the annexation by sending in official troops. The annexation of Crimea by Russia was confirmed by a referendum of independence from Ukraine held on 16th March, which was deemed illegal by the Ukrainian government and the UN, and the Treaty of Accession of the Republic of Crimea to Russia, which was signed by Crimean and Russian representatives on 18th March (Bebler, A., 2015).

b) War in Donbass:

After Russia's annexation of Crimea, and as a reaction against the Euromaidan movement, a series of armed clashes between separatist and pro-Russian groups and the new Ukrainian government took place in the Donbass region, located in the eastern Ukraine and close to the Russian border. Separatists proclaimed the independence of two areas within the Donbass region: the Donetsk and Luhansk People's Republics. Although Russia repeatedly denied its involvement in this armed conflict, dubbing it a 'civil war', both Ukraine and the NATO reported the presence of Russian troops and military equipment supporting separatists in the Donbass region (Council on Foreign Relations, 2020). The conflict has continued intermittently until now, and, according to the United Nations Office of the High Commissioner for Human Rights (OHCHR), it is estimated that around 13 000 people have been killed: at least 3 350 civilians, around 4 100 Ukrainian troops and around 5 650 members of armed groups. Another 29 000-31 000 have been injured (Office of the United Nations High Commissioner for Human Rights, 2020).

In July 2014, the local conflict escalated to an international crisis after flight MH17 was shot down over the Donetsk Oblast region. Although Russia tried to elude its responsibility through an intense disinformation campaign aiming to blame the Ukrainian government, the investigation conducted during 2015 by the Dutch Safety Board and a joint investigation team (JIT) concluded that the aeroplane was shot down by a surface-to-air missile (Dutch Safety Board, 2015). A subsequent criminal investigation conducted in 2016 by international prosecutors of the JIT concluded that the missile was provided by Russia and launched from a territory controlled by Russian-backed separatists. In 2018, the JIT concluded that the missile came from a Russian Army unit, and accused several Russian Army officials and separatist leaders of the murderer of all 298 persons on board (East StratCom Task Force, 2019a).

The case of flight MH17 unleashed one of the largest disinformation campaigns from the Kremlin, in which the Russian media used a large amount of manipulated or directly false news to exempt themselves from any type of responsibility. Pro-Kremlin narratives regarding this event occur even today, as Russia continues to spread false or manipulated information, in which it tries to paint itself as

a victim of an international plot against the country, or continues to argue that Ukraine was responsible for shooting down the aeroplane.[37]

Legal

After the annexation of Crimea, Russia, taking advantage of loopholes in international law, tried to justify its actions using a legal narrative. It attempted to give the appearance that such actions were legally covered, highlighting that each people has the right to decide its own sovereignty. Russia used a discourse analogous to that the EU could use in relation to the rights of minorities and separatist movements in the former Soviet Republics (Allison, R., 2014). Russia took advantage of the illegal referendum in which Crimean citizens could decide whether they wanted to remain part of Ukraine or integrate into the Russian Federation (97 % voted in favour of annexation to Russia) to show the international community that the annexation was justified by the feelings of citizens of the Crimean Peninsula.

Cyberspace

In the case of Ukraine, diverse hybrid components from the digital domain were also deployed. The two most significant are discussed:

1 Cyberattacks.

The following table shows some of the most relevant cyber-attacks during the crisis in Ukraine.

Table 8: Chronology of main cyber-attacks in the Russian-Ukrainian conflict

Date	Description
11.2013	The websites of Ukrainian institutions were targeted by DDoS attacks, as a consequence of the pro-European Euromaidan movement.
18-21.02.2014	DDoS attacks on Ukrainian websites and on Ukrainian Members of Parliament's mobile phones.
07-14.03.2014	Various Russian websites were targeted by DDoS attacks in retaliation for the invasion of Crimea.
16-18.03.2014	DDoS attacks on Ukrainian websites were reported.
24.05.2014	A pro-Russian hacker named *CyberBerkut* hacked the servers of the Central Election Commission (CEC) of Ukraine and infected the election networks with malware.
25.10.2014	Several DDoS attacks and hacks were observed against Ukrainian institutions during the Ukrainian parliamentary election campaign.

[37] Some recent examples of disinformation campaigns related to flight MH17 can be found on the website www.euvsdisinfo.eu:

- The MH17 trial is a politically motivated process against Russia by the United States: https://euvsdisinfo.eu/report/mh17- tribunal-is-a-politically-motivated-process-against-russia-and-dnr/
- There is no valid evidence because the allegations were based exclusively on digital articles: https://euvsdisinfo.eu/report/none-of-the-evidence-of-the-jit-are-valid-all-the -accusation-is-based-on-some-articles-in-the-media/
- The evidence being presented at the trial has been altered or manipulated to blame Russia for what happened: https://euvsdisinfo.eu/report/russian-expert-confirms-new-evidence-mh17-tampered/

23.12.2015	A cyberattack on the Ukrainian power grid left approximately 250,000 inhabitants without power for several hours.

Source: (Baezner, M., 2018)

Among the most significant impacts were the reputational costs of website defacement, the economic costs of denial of service (DDoS) attacks and the need to replace affected equipment following the cyberattacks on Ukraine's electricity grid.

2 Disinformation campaigns.

During the crisis in Ukraine, false information was widely used to add more confusion and aggravate the conflict. Russian television and social networks (mainly Twitter) were the main distribution channels of disinformation campaigns. Russian state TV channels helped to spread the Kremlin's strategic narratives amongst the population, on the one hand focusing their discourse on Western hostility and the existence of secret EU interests in Ukraine, and, on the other hand, deploying the idea that fascism was slowly growing in Ukraine (Cottiero, C. et al., 2015).

A recent study proposed the hypothesis that not only could Russia have used social networks to spread its narrative amongst Russian speakers in Ukraine, but also to gain military intelligence. By gauging public opinion through social networks about the changes in the Russia-Ukraine border after Crimea's annexation, Russia could have determined in which other territories they could have deployed troops without resistance (Driscoll, J. & Steinert-Threlkeld, Z., 2020). Although researchers did not find evidence of data from social networks being used in this way in this case, they did emphasise the potential of real-time data collection and analysis from social networks for repurposing military actions.

Since the beginning of the Ukrainian conflict, Russia has spread numerous false stories through digital means, attributing false actions or activities to the Ukrainian government (or government-sponsored groups), including violent actions such as planting bombs or using firearms against opposition groups (Snegovaya, M., 2015). The most relevant disinformation campaigns were those related to the downing of the flight MH17 (discussed above), which aimed to hide the Russian origins of the attack, and the case of the boy crucified by Ukrainian soldiers in Sloviansk, which was broadcasted through the Russian state-owned Channel One during the war in Donbass (Tomkiw, L., 2018).

Religious affairs

President Putin has progressively replaced the communist revolutionary vision with the values of the Russian Orthodox Church, and has established these values as an essential element of Russian identity, creating a new morality, code, meaning and purpose for Russia (Dalla Mora, M., 2019). In line with this, religious sentiments have also been used by the Kremlin to justify the annexation of Crimea, as this region is a fundamental part of Russian religious and cultural heritage (Coyer, P., 2016).

The Russian Orthodox Church (ROC) has always been massively influential in all the decisions made by Russian leaders, except for during the first decades of the communist revolution. Thus, religion has been a significant factor in Russia's history. After the dissolving of the Soviet Union, the newly formed Russia announced the ROC, the Army, and the state authority to be the pillars of the nation. Even today, the ROC is closely tied to all the decisions made by the Kremlin, including the decisions made regarding external affairs (East StratCom Task Force, 2019b).

Ukraine is a country of plural religious convictions. Ukrainians particularly disliked the power that the ROC exerted amongst other orthodox churches and, even before the country became independent, they believed that the ROC always sided towards the Russians. As a result, in December 2018, the Ukrainian Orthodox Church (UOC) was instituted following the Unification Council held in Kiev, reunifying two of the three orthodox congregations existing in the country (the third remained under

the jurisdiction of the ROC). The new religious institution was granted the Tomos[38] of autocephaly by the Ecumenical Patriarchate of Constantinople, re-establishing its jurisdiction over Kiev, instead of Moscow.

The autocephaly of the UOC limited the Kremlin's ability to influence Ukraine through the ROC, so Russia tried to disparage the new church, going so far as to qualify its creation as a 'CIA operation' (East StratCom Task Force, 2018).

4.4.3. Strategy, tactics and tools to counter the hybrid threat

Ukraine and the international community tried to counter the hybrid warfare developed by Russia using diverse strategies. In the military sphere, Ukraine, once the separatist movements began to act, launched an anti-terrorist operation in response to the destabilisation actions that were taking place (OSCE, 2014). However, this solution proved to be inappropriate, due in part to the poor training that military forces had received, the scarce weaponry they had available and the low morale of troops due to the annexation of Crimea.

At the international level, the EU decided to implement several soft power tools, with the aim of preventing the escalation of tension:

- Creation of the EU Advisory Mission in Ukraine (EUAM). It was set up in December 2014 and aimed to help Ukrainian authorities achieve sustainable reform of the civil security sector through strategic advice and practical support for specific reform measures based on EU rules and international principles of good governance and human rights. EUAM's aid priorities in Ukraine are:[39]
    - Human resource management to ensure that skilled people are deployed to help develop the necessary reforms.
    - Strengthen aid for criminal investigation to combat organised crime and corruption.
    - Help Ukrainian authorities to maintain peace and public order while preserving the right of citizens to express their disconformity with public action.
    - Advise on the delimitation of competencies, to clarify the functions of each public institution and avoid overlaps and excessive bureaucracy.
- Imposition of restrictive measures against Russia (European Council, 2020a):
    - Diplomatic measures: cancellation of the EU-Russia summit in 2014 and regular bilateral summits with Member States. EU countries also agreed to suspend negotiations on Russia's entrance to the OECD and the International Energy Agency (IEA).
    - Individual restrictive measures: 170 individuals and 44 entities were subject to asset freezes and travel bans, due to their responsibility in undermining the territorial integrity, sovereignty and independence of Ukraine.
    - Restrictions on economic relations with Crimea and Sevastopol: import bans on goods from that region; restrictions on trade and investment; prohibiting supply of tourist services; and export bans on certain goods.

[38] *Tomos*, is a decreee issued by heads of particularn Eastern Orthodox Churches on such issues as the level of dependence an autonomous church may enjoy from its mother church.

[39] https://www.euam-ukraine.eu/our-mission/our-priorities/

- Economic sanctions: applicable to trade with Russia in certain economic sectors (financial, energy and defence).
- Economic cooperation restrictions: the European Investment Bank (EIB) suspended the signing of new financing operations in the Russian Federation; the implementation of EU regional and bilateral cooperation programmes with Russia were reassessed and other economic cooperation programmes were also suspended.

The Organisation for Security and Co-operation in Europe (OSCE) created the OSCE Special Monitoring Mission to Ukraine, whose tasks were to observe and report on the situation in Ukraine from a neutral perspective and facilitate dialogue amongst all parties involved.

In March 2014, the European Commission approved a first aid package with various concrete measures of economic and financial assistance to Ukraine (European Commission, 2014b). Since then, the EU and their Member States have provided financial and humanitarian aid worth €1 billion (European Commission, 2020e).

The European Parliament has also played a key role in supporting and promoting the Ukrainian people:

- Reiterating its commitment to the sovereignty and territorial integrity of Ukraine within its internationally recognised borders, and with its choice to follow a European path (European Parliament, 2016b).
- Pointing out that restoring Ukrainian control over the peninsula is one of the prerequisites for restoring cooperative relations with the Russian Federation (European Parliament, 2016a).
- Calling on Russia to release all Ukrainian citizens illegally and arbitrarily detained, both in Russia and in the occupied territories of Ukraine; to stop issuing Russian passports to all Crimean people; to stop systematically intimidating local citizens opposed to the annexation of Crimea; to investigate all cases of human rights violations; to respect the fundamental freedoms of all residents, including freedoms of expression, religion or belief and association; and the right to peaceful assembly (European Parliament, 2017b).
- Proposing the amendment of Regulation (EC) No 539/2001 to allow Ukrainian citizens to be exempt from the requirement to have a visa when travelling to EU Member States (European Parliament, 2017a).
- Proposing the application of the EU Association Agreement with Ukraine (European Parliament, 2018a).

Another soft power measure implemented by the international community was the suspension of Russia's participation in the G8 group of leading economies in March 2014 (Acosta, J., 2014).

In the field of digital communications, several initiatives were launched to combat pro-Russian disinformation. One of the most relevant was the fact-checking website StopFake, created by students, graduates and lecturers of the Kyiv Mohyla Journalism School (StopFake.org, 2020). Although the site was created with the intention of denouncing Russian propaganda on the Ukrainian conflict, it has become an information hub for analysing all types of Kremlin disinformation campaigns. The site is currently researching, fact-checking, translating and disseminating information about Russian propaganda in 13 languages.

4.4.4. Impact and consequences

Prior to its intervention in Ukraine, Russia had already assessed the economic sanctions and military responses that could be triggered as a result of such intervention. Nevertheless, after balancing the possible costs and the potential benefits, it concluded that it was worth acting as it did against the former Soviet Republic (Lázaro, A., 2014). Russia did not hesitate to use hard power tools, in both a covert and overt manner, when all other soft power measures (economic, diplomatic, informative) did

not ensure its interests. Instead, it considered that the benefits of such actions would come before any sanction imposed in the international arena (Stratpol, 2016).

Although the annexation of Crimea remains unrecognised under international law, there is wide consensus that this situation cannot be reversed in the short and medium term (Sasse, G., 2017). After the imposition of sanctions, economic ties and diplomatic relations between the West and Russia deteriorated to a point comparable only to the end of the Cold War.

The main consequences of the crisis in Ukraine at the international level can be summarised as follows (Stratpol, 2016):

1. To a large extent, Russia's narrative was able to alter the international community's political sentiment towards Ukraine, painting it as a country without the capacity to protect its people and portraying it as a failed, fascist state.
2. Russia blocked most of the international community's efforts to manage and attempt to solve the Ukraine problem, using its position in the permanent UN Security Council. Russia vetoed any effort to deploy a UN peacekeeping mission in Ukraine, which resulted in the OSCE being the only international organisation with sufficient supervisory capacity present in Ukraine.
3. Although Russia tried to improve its image with an expensive public diplomacy campaign, taking advantage of the Sochi Olympic Games (Marcin, M., 2016), the annexation of Crimea greatly damaged its public image and its official discourse. Russia never accepted the role of aggressor, and instead presented itself as a victim of the aggressive policies of the West (mostly promoted by NATO).

In the field of strategic communications, the Russian intervention in Ukraine triggered the launch of several fact-checking initiatives aimed at debunking Russian propaganda. In fact, the creation of the East StratCom Task Force by the European Union External Action Service was indirectly linked to the Russian-Ukrainian conflict, as its launch was one of the conclusions of the European Council held on this conflict in March 2015 (European Council, 2015).

4.4.5. Conclusions of the case

As described above, the beginning of the conflict can be established at the Euromaidan protests from November 2013. The actions that the Kremlin has used in this conflict have been multiple and very diverse, but it has always refrained from employing military action from its regular armed forces.

The preparation of the hybrid attack against Ukraine, that is, the identification of Ukrainian weaknesses was largely based on the Russian Federation's traditional foreign policy activities. Russia developed a large number of elements to undermine Ukrainian integrity, from intelligence operations, stimulation and logistical support for the establishment of pro-Russian volunteer forces, use of electronic warfare systems (computer attacks), proselytising in the field of social networks, orchestrated use of media disinformation campaigns and propaganda through digital means, as well as economic pressure and blackmail.

The aggression started by Russia against Ukraine was a relative success, because despite the threats at an international level after the illegal annexation of Crimea, Russia does not seem to have changed its attitude regarding both actors (Ukraine and Crimea).

An important lesson to be learned from the events in Ukraine is that an adequate legislative framework and enforcement mechanisms, as well as clear communication strategies, must be established to efficiently counteract separatism, unconstitutional acts, hate speech and other actions that can serve as the roots for hybrid war attacks from abroad.

4.5. Case 5: Disinformation campaigns against NATO operations in Lithuania

In the context of NATO operations in Lithuania (the Enhanced Forward Presence mission), 40 designed as a deterrence campaign against Russian pressure on Baltic countries' borders, diverse disinformation campaigns against NATO soldiers tried to undermine local citizens' trust in such operations. The rapid and straightforward response of the authorities concerned is one of the best recent examples of a successful communication strategy to counter a hybrid threat.

This case addresses the analysis of a hybrid threat where the main component used was disinformation campaigns. The goal of the hybrid threat was destabilising the work and eroding the image and reputation of an international organisation, NATO, whose mission was to reinforce the security of the Lithuanian[41]-Russian border.

This case shares similarities with a previous case that took place in Germany. Both cases refer to disinformation campaigns about similar facts (alleged teenage rapes) and involve, directly or indirectly, the German authorities. The comparison of the response measures adopted in each case will allow the key elements in effectively countering disinformation campaigns to be identified.

4.5.1. Geopolitical context

After Russia's illegal invasion and annexation of the Crimean Peninsula and the city of Sevastopol in Ukraine, concerns about the Russian threat increased in the Baltic countries. Estonia, Latvia, and Lithuania were under the influence and domination of Russia for several periods during the last century. The Baltic countries, along with Poland and Ukraine, were historically connected and sharing borders with Russia. Now, they are the main objectives of the Russian influence strategies in Europe, and the West in general. However, following their independence from Russia, the three Baltic countries developed a foreign policy of alignment with the European Union and the USA, which led them to join the EU and NATO in 2004.

In the context of growing Russian pressure, highlighted in the national threat assessment reports from recent years (Ministry of national defence & State security department of the Republic of Lithuania, 2020), Lithuania asked for help at the NATO Wales Summit (2014) and at the NATO Summit in June 2016, which took place in Warsaw (Supreme Headquarters Allied Powers Europe, 2018). At this last Summit, the Enhanced Forward Presence (EFP) mission was approved. The aim of the EFP mission was to strengthen the security of Estonia, Latvia, Lithuania and Poland by deploying battlegroups from NATO's allies. It consisted of a deterrence mission to tackle Russian pressure in the region. In particular, the force under rotation deployed in Lithuania was led by Germany with the contribution of Belgium, Croatia, France, the Netherlands and Norway (Lenoir-Grand, R., 2017).

4.5.2. Features of the hybrid threat

Along with NATO's mission (Enhanced Forward Presence), Lithuania continued reinforcing its defence capabilities to face the Russian threat. Therefore, Lithuania sought to strengthen the ties with the USA in terms of military cooperation. On 14th February 2017, the Lithuanian Parliament (Seimas) ratified the Defence Cooperation Agreement with the USA. Until then, the presence of USA's troops had been under NATO legal framework (Trembo, S., 2017).

The same day, after the ratification, the Chairman of the Seimas and some local media outlets received an email stating that a group of German-speaking men raped a girl from an orphanage in the city of Jonava, near the position of the German soldiers participating in the EFP mission. While local pro-

[40] https://shape.nato.int/operations/enhanced-forward-presence

[41] NATO member.

Russian media outlets in the region (Vesti.lv and Baltnews.lt) gave credibility to the information and published the news, the main Lithuanian media outlets reacted by dismissing the information (Andriukaitis, L., 2018).

The Lithuanian police' investigation found out that the email was false, and the rape did not happen. In addition, the police concluded that the email came from a country outside of the EU. As a consequence, the prosecutor's office started a criminal investigation into the false report to clarify responsibility for it (Sytas, A. et al., 2017).

Reactions to the information attack were varied. Lithuanian public officials did not blame anyone and referred to the open investigation of the case. Meanwhile, NATO officials pointed at Russia as the most probable source of the false information. Lithuanian and NATO representatives agreed that the email was a deliberate attempt to spread false information in order to disrupt and create instability between NATO and Lithuania (DW, 2017). However, the disinformation campaign was addressed quickly, and it had no impact on Lithuanian media and society.

The alleged rape was not the only disinformation campaign against the NATO troops stationed in Lithuania. In March 2017, a new email was sent to members of the Lithuanian parliament's Committee on National Security and Defence, accusing the commander of the NATO troops, Lieutenant Colonel Christoph Huber, of being a Russian agent (Stern, D., 2017).

The Atlantic Council's Digital Forensic Research Lab[42] conducted interesting research into the online coverage of the EFP missions in the countries concerned (Estonia, Latvia, Lithuania, Poland and Russia). The research concluded that the EFP missions had triggered a relevant number of hostile posts and articles, most of them based on false information, around four main narratives: (1) the Baltic States are paranoid or Russophobic; (2) NATO is unwelcome; (3) NATO cannot protect the Baltic States; and (4) NATO is the aggressor (Nimmo, B. et al., 2017). The disinformation campaigns described above are clearly aligned with the pro-Russian narratives that try to discredit NATO work supporting the Baltic States in general, and Lithuania in particular.

4.5.3. Strategy, tactics and tools to counter the hybrid threat

Stakeholders have developed coordinated strategies to counter the effects of disinformation campaigns.

Lithuanian authorities

The strategy used by the Lithuanian authorities to debunk the false information can be divided into three phases:

- First, armed forces, media outlets and the government put the information in quarantine and pointed to it as a possible case of disinformation, preventing it from spreading through social media;
- second, an investigation was quickly launched by the Lithuanian police to clarify the origin and veracity of the emails. The investigation rapidly concluded that the accusations were false;
- and third, the contribution of citizens, whose awareness reduced the chances of the disinformation campaigns succeeding (Schultz, T., 2017).

The success of the responses to the fake rape story and the false accusation about the commander of NATO forces of being a Russian agent was a result of the experience and preparation of the agents involved, as well as their rapid reaction. According to the Defence Ministry Spokeswoman at that time, Lithuanian authorities expected attacks of this type around the time of arrival of EFP troops. She also

[42] https://medium.com/dfrlab

stated that this kind of threat was detected more than a decade ago, and counter-propaganda measures were taken. Once the false stories were detected, armed forces, police, government institutions and NATO were warned. The Spokeswoman also pointed out that Lithuanian citizens' awareness about disinformation was one of the main keys to the successful response, as they did not contribute to spreading the false information. (Schultz, T., 2017).

In the field of awareness-raising initiatives, fact-checking tools played a relevant role. In this sense, several fact-checking outlets has been developed in Lithuania in recent years. For instance, Debunk.eu[43] is a fact-checking initiative where the main media outlets, fact-checkers, IT professionals and StratCom units of the Ministries of Foreign Affairs and National Defence and the armed forces cooperate to counter disinformation campaigns (Debunk, n.d.).

Another key point in Lithuania's response to these attacks was the awareness of politicians, police and Army representatives about Russia's role as a major threat to the national security in the Baltic countries. As mentioned above, the National Security Strategy recognised Russia's capacity to endanger Lithuania via non-military means. Along with conventional military power, the document also considered information war as a threat which could lead to disruption of and disaffection with state's institutions, democracy and national defence. (Ministry of National Defence of the Republic of Lithuania, 2017). Even more clear and explicit was the National Threats Assessment 2019 (State Security Department of the Republic of Lithuania, 2019), mostly focused on Russian threats, as well as the three manuals of civil resistance (2014, 2015, 2016) in the case of military occupation of Lithuania. The last version of the manual, as well as the documents mentioned above, identified neighbouring Russia as a possible nation invader (Aleksa, C. et al., 2016).

German authorities

Germany was the second most involved country in the disinformation campaigns, as the soldiers accused of rape were German, as well as the accusation that the NATO troops commander was a Russian agent. Additionally, the disinformation campaign against the German soldiers came a year after a similar case of an alleged rape in Germany, the *Lisa case*.

The Lisa case

On 11th January 2016, the family of Lisa F. reported her missing. Lisa appeared thirty hours later. The Russian media outlet First Russian TV claimed that the girl, from a Russian speaking family, was raped by several migrants of Arab origin during the hours she was missing. Quickly, the foreign Russian media outlets Sputnik, Russia Today (RT), and RT Deutsch issued further coverage of the incident. The story also spread through social media, especially on posts from right wing and xenophobic groups (Treverton, G. et al., 2018).

German police issued a report soon after Lisa's reappearance clarifying that she had not been raped and confirming that the earlier reports were false. Due to her young age, special safeguards regarding her privacy were applied, and the local authorities prevented the information going public. However, the hoax had already spread through social networks and caused widespread impacts on Russian-speaking Germans and far right sectors, leading to street demonstrations against the German government and its policy of accepting immigrants or refugees from Arab countries. The German mainstream media reported on these events and spread the news nationwide while the Russian Foreign Affairs Minister, Sergey Lavrov, encouraged demonstrators, claiming the German legal system had failed because of its political correctness (Janda, J., 2016). This case was later seen by German authorities as a Russian attack, a response to Germany's role as the main supporter of Ukraine in its conflict with Russia (Meister, S., 2016).

[43] https://debunk.eu/

Although both cases had different backgrounds, the lessons learnt after the *Lisa case* allowed Germany to more adequately address the false accusations that German soldiers committed rape in Lithuania.

As the German Federal Academy for Security Policy recognised with regards to the *Lisa case*, 'since the German Government was structurally unable to swiftly react to the unfounded allegations, the case got disproportionate national and international attention' (Janda, J., 2016).

In the Lithuanian case, the Ministry of Defence and the Ministry of Foreign Affairs led the German response, seamlessly coordinated with the other stakeholders (Lithuania and NATO). It allowed false accusations to be debunked before they could be spread through social networks, where they would have been virtually uncontrollable, and could have caused similar damage to the *Lisa case* in terms of national reputation.

While a lack of coordination between authorities at different levels (local, regional and federal) and relevant delays in responding to the false accusations contributed to magnifying the impact of the *Lisa case* on social networks and in the mass media, in this case federal German authorities reacted promptly, asking Lithuania and NATO for all the information needed to debunk the false story and limit its effects.

After countering these disinformation attacks, Germany implemented new measures aimed at addressing new potential hybrid threats based on digital means. Two months after the attacks, the Cyber and Information Space (CIR) unit was created within the *Bundeswehr* (German Army), unifying all Army units in charge of cybersecurity, military reconnaissance and psychological warfare (Gotkowska, J., 2017).

In September 2018, the German Chancellor Angela Merkel visited Lithuania and had the opportunity to speak directly to the German troops involved in the EFP mission. In her speech, Angela Merkel recognised the exposure to Russian hybrid threats and highlighted the ongoing work done by the CIR to tackle them (Agence France Presse, 2018).

A year later (2019), the Chief of Defence in Germany, General Eberhard Zorn, stated that German troops in Lithuania were being instructed on how to use their smartphones and social networks to avoid cyberattacks and information theft. He also pointed out that German soldiers were one of the main targets of hybrid threats. Since the EFP mission started in Lithuania in January 2017, leaded by the German Army, there have been many more cyber and disinformation aggressions against German troops in addition to the first one analysed in this chapter (Baltic News Service, 2019).

4.5.4. Impact and consequences

In general, disinformation attacks carried out by state or non-state actors aim to produce confusion and instability in target societies or environments. In the Lithuanian case, the objective was to create distrust amongst the population towards German NATO soldiers, who were deployed in the country to deter Russia. The ultimate goal was to destabilise and harm the cooperation between Lithuania and NATO in security matters. As NATO's Assistant Secretary General for Emerging Security Challenges said: 'it really was supposed to affect the perception about the presence of German troops within the EFP framework in Lithuania. It was supposed to affect morale; it was supposed to affect everything – the operational functioning' (Schultz, T., 2017).

Because of the similarities, attackers may have expected similar consequences as in the *Lisa case*. The false information was quickly spread by pro-Russian media outlets and by specific groups on social media platforms, drawing the attention of German mass media and fuelling the protests by outraged Russians and far-right extremists in Germany, encouraged by the Russian Foreign Affairs Minister, Sergei Lavrov. (Treverton, G. et al., 2018). But, due to the failure of the disinformation attack, thanks to the coordination between all the parties involved and their rapid reaction, it could be argued that the image of Lithuania and NATO was reinforced by successful resolution of the crisis.

4.5.5. Conclusions of the case

Pro-Russian disinformation campaigns against the presence of foreign soldiers under NATO mandate on Lithuanian soil include most of the characteristics that allow such campaigns to be classified as hybrid threats. Disinformation campaigns were launched in a timely manner, shortly after the arrival of the troops led by Germany. They were launched through several channels, from email campaigns to key Lithuanian representatives and media outlets, to posts and articles on online platforms. The attackers fabricated a false narrative around one of the most nefarious crimes, rape, appealing to the citizens' most profound emotions and feelings to create mistrust and rejection of German soldiers. In the end, what pro-Russian attackers sought to do was undermine a sovereign decision of Lithuania (the request for help to NATO, latter resulting in the EFP mission), blaming NATO soldiers for crimes that were never committed and thus creating bias towards them.

The response measures implemented were focused on swiftly debunking false information and impeding its spreading through online means. Proper coordination between the stakeholders involved (Germany, Lithuania and NATO) was the essential feature that allowed the threat to be addressed in a swift and effective way. Other measures related to prevention were implemented, like the training provided to soldiers to properly manage their smartphones and social network profiles in order to avoid cyberattacks and information theft. However, this case particularly stands out due to the coordinated and prompt response, especially when compared to the deficient communication management of previous cases, such as the *Lisa case*.

It is worth noting that prevention measures adopted by Lithuania regarding raising awareness amongst citizens about Russian disinformation were also very effective, as Lithuanians were capable to detect and reject false information related to this case.

4.6. Case 6: Russian electronic warfare during Zapad 2017 military exercises

The Russian army has always been convinced that the success of its military operations depends not only on how well equipped its members are, but also on well-planned and executed operations. This is why Russia has been preparing for possible military conflicts of all kinds for years (Norberg, 2018). In relation to this preparation, every four years Russia carries out the Zapad's military exercises, which have involved elements of technologic and electronic warfare since 2009 (Petraitis, D., 2019).

The Zapad 2017 exercises were more than military manoeuvres 'of a strictly defensive nature', as Russian Defence Minister Sergei Shoigu claimed (AFP, 2017). On the contrary, it was an example of strategic deterrence: displaying Russia's growing military power and willingness to use it as an instrument of intimidation and coercion over neighbouring countries, NATO and the EU, to foster fear and unease.

Meanwhile, in addition, Moscow used a narrative in which it presented itself as a victim of a conspiracy to undermine its values. It initiated counterattack by denouncing the West's fantasy of starting an armed conflict against Russia (European Journalists Association, 2017). The fear that Russia might start a war was especially evident in Poland, Lithuania and Ukraine, where diverse theories on how Russia could exploit troop movements during Zapad exercises to gain some kind of military advantage were developed (Center for European Policy Analysis, 2017).

During these Zapad exercises, the accumulation of reports from Western media and even official statements succumbed to a spiral of alarm and speculation. Instead of raising awareness, some media outlets increased anxiety by overreacting, thus magnifying the intimidating potential of the exercise (Lasconjarias, G. & Dyčka, L., 2017). This is why the Zapad 2017 exercises were more than mere military exercises, and instead became a hybrid threat to neighbouring countries.

4.6.1. Geopolitical context

Zapad military exercises are some of the most realistic trainings carried out by the Russian army, in which simulations that are very close to reality are carried out, with the aim of testing the army's capabilities in the case of an hypothetical armed confrontation with the West (Johnson, D., 2018).

Zapad training is usually carried out in three phases (Petraitis, D., 2019):

- The first involves basic entrenchment and defence exercises.
- The second phase aims to protect the achievements of the previous phase and try to extend the control zone. In this stage, strategies necessary to stabilise the conflict or even to conclude it are employed.
- The third phase is called *the mass phase*, when the main activity is to use all the resources available to defend the objectives achieved. This may even involve the use of nuclear weapons if all other defensive techniques fail.

During every Zapad exercise, there are rest periods, used to:

- Reinforce forces/get teams to execute the next task/mission objective.
- Reflect on resources and strategies to persuade the opponent to resolve the conflict through non-military means.

The Zapad 2009 exercises were the first exercises after the military reforms in Russia. At that time, Russian forces and their capabilities were weak and limited. Military leaders thought that such weakness might give their opponents a chance to attack Russia. The Zapad 2009 exercises were mainly a theoretical simulation of the application of tactical nuclear weapons (Petraitis, D., 2019). As Dmitry Medvedev (President of Russia at the time) pointed out, 85 % of the military equipment was obsolete or unusable (Petraitis, D., 2019, p. 10).

Subsequently, in March 2013, the military exercise Zapad 2013 took place, shortly after Russian Army General S. Shoigu was appointed defence minister. The Zapad 2017 exercise was carried out with the help of the Belarusian Armed Forces and the 1st Russian Guard Tank Army.

These exercises represented more than simple military manoeuvres. They were used as a strategic deterrent tool, in which Russia exhibited its military power and its willingness to use it when the time comes. The exercise was an example of intimidation and coercion (Milosevich-Juaristi, M., 2017a). The main objective of Zapad 2017 exercise was to improve the levels of preparation and integration of various military bodies, and to enhance Russia's nuclear, military and non-military capabilities (Warsaw Institute, 2017).

The Zapad 2017 exercises involved 12 700 soldiers (according to the data provided by Russia), a figure that is not irrelevant. It remained just below the number of 13 000, which the *2011 Vienna Document on Confidence and Security-Building Measures,* drawn up by the *Organisation for Security and Cooperation in Europe* (OSCE), established as the threshold above which the military exercises should be subject to international observation. Russia held onto the fact that the numbers shown were real, and it therefore did not have to provide access to international observers beyond the opening day (Leonir-Grand, R., 2017). Regarding the effective number of military personnel who participated in the exercise, there were always suspicions that many more would participate than Moscow claimed. One of the critics was Tomáš Valášek, a former Slovakian ambassador to NATO, who pointed out that special care should be taken, since in uncertain political times an accidental conflict is more likely to occur (Heath, R., 2017). Also, the NATO Secretary General, Jens Stoltenberg, noted that 'the number of troops participating in

the exercises significantly exceeded the number announced before the exercise; the scenario was different and the geographical scope was greater than previously announced' (Emmott, R., 2017).

4.6.2. Features of the hybrid threat

The main threat of the Zapad 2017 exercises came from the use of elements of electronic warfare. The countries affected by the military exercises were Latvia and Norway:

- Two weeks before the start of the Zapad 2017 exercises, Latvia's western district suffered a seven-hour interruption of its telephone networks. Several studies indicated that it was a collateral damage of an electronic attack from a warship aimed at Swedish military exercises on the island of Öland (Diena, 2017).
- Before the start of the exercises, Norwegian commercial aircraft flying over the Finnmark region of Norway reported a complete loss of GPS signal, which lasted a week. This GPS outage forced the planes to use alternative means of navigation. Several analyses of the signals showed that the interference came from the Russian border region in the East (newsinenglish.no staff, 2017).
- Violation of Lithuanian airspace by two Russian planes, which according to Moscow, was caused by adverse weather, forcing the pilots to take a detour (The Lithuania Tribune, 2017).

Both Norway and Latvia pointed out that the disruptions to their infrastructure were probably side effects of actions taken by the Russian Armed Forces when jamming the systems of their own troops near the border. However, the Latvian Foreign Minister called the incident 'a symbolic political gesture against the Baltic States, which showed that Russia was doing its best to intimidate NATO', and recalled that Article V of the North Atlantic Treaty (which stipulates that an attack on one ally is considered an attack on all allies) could also be invoked in cases of technological warfare attacks (Vikmanis, V., 2017).

In addition to the physical electronic damage suffered by Latvia and Norway, there were also psychological consequences of the Zapad 2017 exercises, such as fear caused by the deployment of strength shown by Russia, and the spread of uncertainty and anxiety in the populations of both countries. Psychological damage could have been even greater if the effects of electronic warfare had affected public infrastructure (NATO StratCom CoE, 2019). Moreover, Zapad 2017 manoeuvres raised the suspicion among Western analysts that Moscow could use them to attack a NATO member country. Russia's lack of transparency about these military exercises encouraged Western media, including even reliable sources, to do its job for it, by circulating speculation and alarmist theories that left Europe alarmed at the prospect of a new military attack. A position which, in turn, was entirely comfortable for Moscow's objectives of generating fear and anxiety amongst Europeans (The Economist, 2017).

4.6.3. Strategy, tactics and tools to counter the hybrid threat

Due to the ambiguous nature of the threat and the significant delay in determining the origin of the aforementioned technological problems with a high degree of certainty, it was not possible to attribute responsibility and respond in a timely and decisive manner.

4.6.4. Impact and consequences

Apart from the damage already identified in Norway and Latvia, and the fear caused to people in neighbouring countries, these exercises led to a serious reflection on the following issues in the international sphere:

- Relevance of electronic warfare in future conflicts: Information-psychological operations (and reflective control) are the backbone of Russian information warfare against the West today. Zapad 2017 became a peculiar mix of intimidation and defence-related rhetoric, thus serving both internal and external purposes. In particular, it is worth noting the increasing priority Russia gave to its electronic warfare capabilities (both offensive and defensive) and how this

element of electronic warfare was also widely tested in various regions of Russia before and during the exercises (Sukhankin, S., 2017).

- Need to improve coordination between security strategies in the countries under Russian influence (Conley, H. et al., 2018).

According to the NATO Strategic Communications Centre of Excellence, deterioration of relations between the Russian Federation and the West mainly affects the way in which events such as territorial violations and military exercises are interpreted. NATO countries should be prepared for disturbing events such as cyberattacks or disinformation attacks, whose authorship is difficult to determine, and which can cause serious ecological, social and political damage. Coherent responses and appropriate strategic communication plans are needed to counteract potential damage of those military exercises (NATO StratCom CoE, 2019).

4.6.5. Conclusions of the case

As described above, the elements of hybrid threats used in this case were mainly three: technological disruption, invasion of airspace and military pressure, with the latter undoubtedly being the most important, aimed at intimidating neighbouring countries and NATO members. While Russia's overt objective regarding the Zapad exercises was to improve its defence capability, they were also covertly aimed at spreading fear and anxiety amongst neighbouring populations.

From Moscow's perspective, the justification for this type of exercises was based on the fact that Russian security on its Western borders was deteriorating as a result of increased NATO activity in Eastern Europe countries (improving the infrastructure of their seaports, airfields and other military facilities), even if these modest preparations could not pose a real threat to Russia.

The strategic communications made by the Western media were unfortunate, as they effectively and unintentionally collaborated with Russia's objectives of conveying and amplifying its message of intimidation. The alarmist information spread by Western media could, in turn, contribute to their sources being discredited and making them less reliable in the future.

4.7. Case 7: Disinformation attacks in the Catalan issue

The political conflict that occurred in Spain in 2017, climaxing in the Regional Government of Catalonia's attempt to push for the region's independence, was fuelled by hybrid tactics including disinformation campaigns and foreign influence. Social networks became an essential tool in spreading false information aimed at exacerbating independentist sentiments and portraying Spain as a non-democratic state, seeking international support for secessionists. This case describes how strategic communications were used by both parties and the relevant role that digital technologies played during the political crisis.

4.7.1. Geopolitical context

After years of fuelling independentist sentiments amongst Catalonians, the government of the Autonomous Community of Catalonia (known as the 'Generalitat') organised a referendum which was intended to solicit the opinion of the citizens of this Spanish region on their desire for Catalonia to become an independent state. The referendum was to take place on 1st October 2017 (1-O).

The Government of Spain, understanding that such a claim was contrary to the Spanish Constitution, lodged an appeal with the Constitutional Court. On 7th September 2017, this court cautiously suspended the Catalan law calling for the referendum and warned the 948 Catalan mayors and 62 officials of the Catalonian Government that they could not participate in organising the referendum. Likewise, the General State Prosecutor's Office presented a complaint to the Constitutional Court claiming disobedience, prevarication and misappropriation of public funds by the President of the

Catalan Parliament, the members of the Bureau who voted in favour of processing the Referendum Bill, the President of the Generalitat and all members of his Government, by considering that law, and its associated expenses, unconstitutional.

Despite all the warnings, the Catalan Government decided to go ahead with the referendum, which finally took place without due legal guarantees, in an atmosphere of tension that included certain episodes of violence. On the planned date, Catalan citizens could respond 'yes' or 'no' to the question: Do you want Catalonia to be an independent state in the form of a republic?

Social tension and division between those in favour of and those against the referendum being held was significantly widened as a result of the false news that was spread before, during and after the 1-O.

4.7.2. Features of the hybrid threat

Several components of hybrid threats were used by the Catalonian independentist movement and its foreign supporters to achieve its goals:

- To present the holding of the referendum as the right of Catalan citizens, despite it violating the Spanish Constitution;
- to present Spain as an anti-democratic and oppressive state that prevents Catalan citizens from exercising their democratic rights;
- to internationalise the conflict.

The most relevant hybrid tactics are described in the following sections.

Foreign influence

Diverse foreign actors supported the independentist movement before and during referendum. One of the most significant supporters was Julian Assange, founder of Wikileaks. Indeed, he became one of the most influential figures on social networks in relation to the Catalan conflict. Although Assange had not shared any message on Twitter on the subject prior to the suspension of the Catalonian Referendum Bill by the Spanish Constitutional Court, from that day until the date of the referendum he shared around 48 messages in English, Spanish and Catalan. All of them supported, directly or indirectly, the claims of those who encouraged the independence of Catalonia. His allegations included spreading the idea that the use of violence by the police in charge of preventing the consultation was extreme, even comparing Spanish police action to the repression by Chinese authorities at Tiananmen Square.

In addition, on 27th September, four days before the illegal referendum, Julian Assange participated in a video conference in support of Catalan separatist claims. The logistics of this conference were handled by the independence group Universitats per la República and it was broadcasted on a giant screen in Plaça Universitat in Barcelona (Segura, C., 2017).

Another foreign actor involved in the Catalan issue was Russia (Alandete, D., 2017c). Russia has been promoting secessionist movements to destabilise other countries for years. One of the first international events where the Catalan separatist movement could express its claims internationally was the congress entitled 'Dialogue of nations and the right of peoples to self-determination and the construction of a multipolar world', promoted by the Russian government in 2015 and 2016, which brought together representatives of independence movements from all over the world (Luhn, A., 2015).

One of the first pieces of false information about Catalonia that expanded internationally ('An independent Catalonia will recognise that Crimea is Russian') [44] was posted by several media outlets such as Sputnik, quoting the Russian media outlet Izvestia as the alleged source of the information.

According to the National Cryptologic Centre, (a body attached to the Spanish National Intelligence Centre), 'the presence of activists sponsored by Russian institutions in the media, expression of the conflict derived from the situation created in Catalonia during 2017 as a consequence of the distancing of certain Catalan autonomous institutions from the constitutional legality in force, seems to have been demonstrated' (CCN-CERT, 2018).

Investigations carried out by the Ministry of Defence had also reached the same conclusions (Alandete, D., 2019). They were ratified by Jens Stoltenberg, Secretary General of NATO, who confirmed interference from Russian organisations (RTVE, 2018).

Janis Sarts, Director at the NATO Strategic Communications Centre of Excellence, pointed out that the ultimate intention of the Russian networks is not to encourage Catalonia's independence but to deepen divisions in society in order to weaken the EU and NATO itself. Their aim is to confuse and aggravate existing problems in society, not to achieve a result that favours one or the other (Alandete, D., 2019). In the same vein, another report noted Moscow's aspirations to foster disagreements in Catalonia in order to weaken a NATO member (Baqués, J., 2018).

Disinformation

In the weeks prior to the illegal referendum, the East StratCom Task Force, through the website euvsdisinfo.eu, showed an increase in disinformation campaigns aimed at aggravating the crisis in Catalonia, triggered by various Russian media outlets. According to the East StratCom Task Force, mentions of Catalonia in Russian disinformation media outlets had increased from 4 to 241 per week (Alandete, D., 2017b).

The pro-independence narrative's main argument when creating disinformation was that contemporary Spain is in fact a whitewashed substitute for Franco's regime, and has inherited its authoritative and oppressive ways, an idea that Russian media outlets such as Sputnik or RT constantly repeated during 2017.

The alleged use of violence by the Spanish Government to suppress the independentist movement was another recurrent topic for disinformation. For instance, on 28th October 2017, Russian media outlet RT published this news: 'Tanks in the streets of Barcelona: Spain and Catalonia on the verge of a violent end'. [45] A few hours after its publication the news triggered 11 800 Facebook interactions, an impact three times higher than the average for information from RT on this platform. On Twitter, in turn, RT's profile was shared up three times more than usual, which caused some 12 000 people to react to that news, sharing it or commenting on it. [46]

Police interventions, in compliance with the sentences from the courts, were the most delicate moments of the day of the illegal referendum. RT drew on this situation to build false media coverage with the title: 'HARD VIDEOS: Brutal police repression against Catalan referendum voters'. This information achieved 11 400 interactions on Facebook and 3 300 on Twitter (Alandete, D., 2019).

According to what the General State Prosecutor's Office expressed in its accusation during the trial against those responsible for organising of the referendum, the figure 'close to a thousand injured' provided by the Generalitat de Catalunya in the day of the illegal referendum 'was manipulated to

[44] https://sputniknews.com/world/201609281045773918-catalonia-recognize-crimea-russian/

[45] https://actualidad.rt.com/actualidad/253812-espana-cataluna-violencia-conflicto

[46] These measurements were conducted with the service NewsWhip Analytics, which measures news interactions on five social platforms, including Facebook and Twitter (Alandete, D., 2019).

magnify the police repression, since it has been proved that in a high percentage of cases the medical attention received was exclusively as a consequence of dizziness and anxiety crisis, and not for injuries caused by the police officers' (Supreme Court Prosecutor, 2018, p. 116). In fact, the Supreme Court Prosecutor's Office stated that 'only four people were admitted to hospitals: two slightly and two seriously injured' (Supreme Court Prosecutor, 2018, p. 116). During the trial, the former head of the Catalan Public Health Service, David Elvira, explained to the court that on the day of the referendum, only five people were severely injured, representing 0.5% of the 991 people who received care throughout Catalonia on that day (Berbell, C., 2019).

Bots and social networks

Distribution of disinformation is usually done through social networks, using automated profiles or bots, and using mechanisms to mask their geographical origin, such as proxies and VPN servers. This was proven in the Catalan issue thanks to the tool Hamilton 68, [47] created by the Alliance for Securing Democracy. According to this tool, which monitors the daily information released by six hundred Twitter accounts managed from Russia, a 2 000 % increase in activity related to Catalonia was detected on the day of the referendum, using, especially, the hashtag #Catalan.

A study on bot activity over the days leading up to and after the Catalan referendum was published in November 2018. It analysed 3.6 million messages on Twitter, published by 523 000 users between 22nd September and 3rd October 2017, with the hashtags #Catalunya, #Catalonia, #Catalogna, #1Oct, #votarem, #referendum and #1O. The study showed that 33 % of users were bots aimed at spreading negative content and inciting hatred and confrontation (Stella, M. et al., 2018).

According to another study, between 29th September and 5th October 2017 news and information referring to Catalonia produced by RT and Sputnik (in Catalan, Spanish and English) was shared a total of 47 964 times through social networks, with an audience of up to 125 million users. This is ten times more than the information produced and distributed by the Spanish public media, RTVE and the EFE public news agency (Lesaca, J., 2017). The study concluded that only 9 of the 100 most active accounts sharing RT and Sputnik content seemed to follow a human behaviour.

Other studies published by prestigious entities, such as the Elcano Royal Institute, insisted that the presence of Catalonia on social networks increased by 2 000 % in September 2017. For example, some messages from Julian Assange criticising the attitude of the Spanish Government were retweeted 60 times per second, actions that could only be carried out by bots (Milosevich-Juaristi, M., 2017b).

4.7.3. Strategy, tactics and tools to counter the hybrid threat

The events around 1-O revealed that without a specific strategy to counteract digital interference, democratic states are at serious risk. Some specialised journalists have pointed out that the Spanish Government's narrative was absent from the conversation on social networks. The Spanish public media, including radio, television and the news agency EFE, did not even have a planned information strategy to counter the independentist discourse (Alandete, D., 2019). As a result, the independentist narrative won the first battle of disinformation in the days leading up to 1-O, mainly at the international level. Although the Spanish Government was slow to react to the challenge posed by the Catalan independentist movement in the realm of communication, it finally implemented several tools to counter future hybrid threats.

After the Catalan crisis, the Spanish government defined diverse measures aimed at preventing and counteracting the impact of disinformation campaigns and cyberattacks, putting both issues on the political agenda. On 13th December 2017, the creation of a Cybersecurity Operations Centre was announced to protect the General State Administration's computer networks from cyberattacks,

[47] https://securingdemocracy.gmfus.org/hamilton-dashboard/

although the fight against false news on social networks was not specifically mentioned amongst its responsibilities (Spanish Government, 2019).

In light of the upcoming elections, in March 2019, the Spanish government launched a unit against hybrid threats, with early response procedures to help to mitigate both cyberattacks and disinformation. Experts from the Department of National Security, the Secretariat of State for Communication and the most involved ministries led these efforts. Evidence of the existence of distorted messages that aggravated the Catalan crisis and the certainty that the elections could constitute a fertile juncture for distortion meant the level of alert was raised, and encouraged the creation of the aforementioned body (Abellán, L., 2019).

In April 2019, the Spain's latest National Cybersecurity Strategy addressed the problem of disinformation for the first time (Spanish National Security Department, 2019).

In the legislative field, Spain has adopted measures to combat disinformation, such as the Royal Decree-Law promulgated at the end of 2019, which included tackling risks derived from false information amongst its objectives.[48] The most recent legislative attempt to deal with disinformation in Spain was the 'Action Procedure against Disinformation' (Ministry of the Presidency, Relations with the Courts and Democratic Memory, 2020). Approved by the National Security Council, it has served as the basis for creating a national system for preventing, detecting, alerting, monitoring and responding to causes, means and/or consequences related to disinformation. This Action Procedure establishes the necessary instruments to participate in the mechanisms that the European Union has made available to Member States. It also reinforces the capacities for coordinated and joint responses to disinformation campaigns, thus increasing the exchange of information with the bodies and agencies with competence in this matter, through the Permanent Commission against Disinformation.

Finally, in the informational sphere, the former Secretary of State of *España Global* developed a comprehensive communication plan to counter independentist propaganda between 2018 and 2019. It comprised the following activities:

- Launching the platform *ThisIsTheRealSpain*,[49] aimed at promoting Spain's strengths, which are categorised into three main pillars: democracy, modernity and citizenship. Based on objective and independent indicators, the platform shows how Spain stands in the international arena in terms of economic and social development, democratic and institutional quality, culture, respect for human rights, etc.
- Coordinated external action through the network of embassies to transmit the Spanish government's narrative regarding the Catalan issue across the world.
- Production and diffusion of several reports and studies debunking independentists messages against Spanish democracy (Global Spain, 2019c).

4.7.4. Impact and consequences

The threat developed by the Catalan separatist movement against Spain before and after the illegal referendum, basically by means of disinformation campaigns, partially achieved its goals. One of them was to increase independentist sentiments amongst Catalan citizens. According to the quarterly barometer produced by the Catalan Government's Centre d'Estudis d'Opinió (a regional public body for sociological studies), the percentage of Catalans that wanted Catalonia to become an independent

[48] The Decree states: 'Among the main challenges that new technologies pose from the point of view of public security are disinformation activities, interference in the processes of political participation of citizens and espionage. These activities benefit from the possibilities offered by computer sophistication to access huge volumes of information and sensitive data'. (Real Decreto-Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones., 2019).

[49] https://www.thisistherealspain.com/

state peaked in October 2017 (48.7 %), the month in which the illegal referendum took place. Moreover, the percentage of people who supported Catalan independence exceeded those in favour of remaining part of Spain in all quarterly barometers until March 2019 (Centre d'Estudis d'Opinió, 2020, p. 12). The independentist narrative managed to convince many Catalans, attracting them with its postulates for almost two years.

However, in the arena of foreign policy, independentists were not successful in their attempt to internationalise the conflict. Apart from some tepid messages of support from countries such as Venezuela (Cembrero, I., 2017), Russia (Alandete, D., 2017a) or South Ossetia (Ministry of Foreign Affairs, 2017), no country in the world recognised Catalonia's independence (Elcano Royal Institute, 2018).

In the European Union, both the Parliament and the Commission positioned themselves in opposition to the illegal referendum. The former president of the EU Parliament, Mr. Antonio Tajani, in a letter addressed to Ms. Beatriz Becerra, MEP, recalled that 'any action against the constitution of a Member State was an action against the European Union's legal framework' and warned that the independence of Catalonia would imply its exit from the EU (Tajani, A., 2017).

Although the Catalan independentist movement did not achieve its fundamental objective, independence, its narrative about the illegal referendum did affect Spain's international image. The images of alleged police violence (most of them false or manipulated) being used to prevent the illegal referendum being held and the Spanish authorities' failure to quickly refute such alleged violence undermined the reputation of Spain abroad.

At the national level, the conflict led to an increase in political and social polarisation, not only in Catalonia but in the whole country. It has also contributed to the fragmentation of the Parliament, hampering the creation of governments based on solid majorities, and the appearance, for the first time in Spanish democracy since 1979, of a far-right political party with parliamentary representation (Vox). As a result of this political instability, and for the first time in its recent history, Spain is currently ruled by a coalition government that has needed the support of Catalan pro-independence parties, and other nationalist parties, to be formed. In order to gain the support of Catalan independentist parties, the coalition government, formed by the Socialist Party and the far-left party Podemos, agreed to enter into a dialogue process with the Catalan Government to analyse its demands for more autonomy.

4.7.5. Conclusions of the case

Disinformation campaigns launched during the events in Catalonia in 2017 had most of the essential components of this type of hybrid threat[50] (manipulated content, attribution of fake content to reputed sources, use of social media, use of bots), but it also included an interesting component in spreading disinformation: the participation of international influencers.[51] Its goals, which were partially achieved, clearly correspond to those of a hybrid threat, particularly (1) erosion of citizens' trust in their institutions (2) generation of mistrust in the democratic system, (3) undermining social cohesion or social models of states, (4) weakening the system of government of its victims, and (5) convincing people of the decay of the political system (both the victims' population and its own).[52]

The measures adopted by the Spanish government to counter the threat were reactive, and focused on two types of action: (1) informative actions, mainly through the España Global agency and diplomatic means and (2) legal actions, with the creation of new public bodies to combat disinformation and cyberattacks, the revision of the national cybersecurity strategy to include

[50] See Figure 4.

[51] An example of this type of influence, in addition to the aforementioned case of Juliane Assange, was Pamela Anderson's position on the Catalan issue. See for example: https://www.pamelaandersonfoundation.org/news/2017/11/6/catalonia

[52] See Chapter 2.1.

disinformation as a real threat, and the production of a new Decree (Real Decreto-Ley 14/2019, de 31 de octubre).[53]

But can the informative actions implemented be considered strategic communications? According to the definition of strategic communications,[54] the Spanish response cannot be fully considered as part of a strategic communication. Its scope was limited as it mostly focused on the international sphere, while it did not include specific targets at the national level. Spanish media coverage was very scarce, and coordination only occurred latter in the process through the foreign service and diplomatic corps, but not with other state institutions. Although communication channels were adequate (diplomatic means, social media and online platforms), the impact on traditional media was small. While other measures adopted do have a long-term preventive objective, the actions taken in the field of communication have been considerably diluted in recent months. In general, the narrative at the national level was mitigated, probably because the minority government formed after June 2018 required the Catalan nationalist parties' votes in the National Parliament.

[53] For a complete taxonomy see Table 4.

[54] See Chapter 3.1.

5. Challenges in effectively countering hybrid threats

Hybrid threats are a serious menace to the proper functioning of democratic systems, in general, and the EU in particular. Promoters of hybrid threats try to exploit the vulnerabilities of EU institutions and Member States with the aim of undermining citizens' trust in such institutions, exacerbating social and political polarisation, deepening social tensions, generating economic losses, or interfering in the political decision-making process. In the end, what promoters of hybrid threats, mainly Russia and more recently China, seek is to weaken the EU and its values, in an attempt to reduce its influence and leadership. Some of the case studies described in the previous chapter are good examples of attempts at undermining the EU.

Although the EU has already implemented different measures to counter hybrid threats, vulnerabilities still persist. These vulnerabilities, and the challenges that they represent, are briefly described in the following sections.

5.1. Lack of harmonised regulation against hybrid threats, particularly against disinformation and foreign influence

The cross-cutting and interconnected nature of hybrid actions limit the effectiveness of the measures used to counter them when taken in isolation. A comprehensive harmonised legal and regulatory framework would make it possible to improve the protection of European institutions and citizens, and should be the foundation of all policies and measures to deal with hybrid threats.

Promoters of hybrid threats take advantage of the disparity of legal regimes in the EU regarding key aspects such as disinformation and foreign influence. They also benefit from the slowness of legal systems in adapting to new phenomena in the digital world. In order to address these challenges, the EU should advance in what could be called legal resilience. This concept may be defined as the capacity of a legal system to resist, recover from and adapt to internal and external disturbances while maintaining its key functions and features, and its capacity to contribute to the resilience of other natural or social systems (Sari, A., 2019). Strengthening EU legal resilience will be key to properly dealing with hybrid threats.

5.2. The effectiveness of the measures depends on the identification of perpetrators

One of the elements that characterise hybrid threats is the difficulty in identifying their origin and attributing responsibility for the attack or threat. Most countermeasures to hybrid threats requires the prior identification of the promoter (foreign or domestic) and the potential local proxies that collaborate in their development. Attributing hybrid threats to their real perpetrators is therefore essential to the success of measures adopted by the victims. It can help identify the ultimate targets of attacks. It can also facilitate public awareness of the nature of threats. But, above all, establishing responsibility for threats is the only way to demand accountability and, if necessary, impose sanctions.

However, attribution is probably the most difficult task when dealing with hybrid threats, especially those that include elements related to cyberspace (cyberattacks, information theft, disinformation campaigns, etc.) (Gressel, G., 2019). Growing technological sophistication and the use of channels such as social networks make identification complex.

5.3. Disinformation is spread through digital means with scarce control by social media platforms

Promoters of hybrid threats are leveraging the enormous potential of digital means, particularly social networks, to spread disinformation among targeted societies. Disinformation campaigns benefit from the nature of social networks, digital platforms that connect audiences without liability for the content, according to the e-Commerce Directive (European Parliament and the Council, 2000). Social networks' tepid attempts at preventing the dissemination of harmful content are limited to illegal categories such as hate incitement, violence, child pornography, terrorism, and cruel and insensitive content. Social networks are allowed to delegate the responsibility of detecting and reporting harmful content to users or, more ambiguously, the 'community', following notice-and-action mechanisms.

While the aforementioned categories are thoroughly explained in the social networks' rules and policies, [55] false information is not considered as harmful content by social networks, and they only include some references to the authenticity of information in specific contexts like election periods, intellectual property or impersonation. Therefore, reporting and taking down false information on social networks is not possible if it does not involve any of the above categories. In addition, as false information is normally very sensationalist and thus more likely to be shared than legitimate information (Peter, M. et al., 2019), 'social media platforms' incentives are not always prioritised to limit disinformation. In some respects, their incentives are aligned with spreading more of it. Tech giants' revenues are generated almost entirely through advertising, which depends on maximising user engagement with the platform (Nemr, C. & Gangware, W., 2019, p. 26).

According to the Special Eurobarometer devoted to analysing attitudes of EU citizens towards the impact of digitalisation on their daily lives (European Commission, 2020d), 48 % of respondents believe social media platforms should be responsible for combatting false information. Europeans give social networks a prominent role in the fight against disinformation. However, their incentives in the digital arena does not seem the most appropriate for such a task. There is an open debate, fuelled by the Executive Order on Preventing Online Censorship of the US President (The White House, 2020) and the proposal to amend regulation for digital services in the EU, called the 'Digital Services Act' [56], about social media platforms' liability for the content spread through them, the protection of the freedom of expression and the role that such platforms should assume in the fight against disinformation, which would require further clarifications about their legal status (Hybrid CoE, 2019).

5.4. Citizens' lack of awareness about the existence and potential damage of disinformation

One of the objectives of disinformation campaigns is to hamper citizens' ability to make informed decisions. Lack of awareness amongst the targeted group stands out as one of the main drivers for disinformation success.

At the European level, awareness about the existence of false information does not seem to be increasing. While there is no evidence of a reduction of disinformation activities between 2018 and 2020, two surveys conducted by the Eurobarometer[57] show a decline in the EU citizens' awareness about the presence of false news or information. The percentage of EU citizens who declared to have found false information or news every day or almost every day has dropped from 37 % to 30 %. The percentage of those who reported finding false information at least once a week also decreased (31 % in 2018; 25 % in 2020). On the contrary, the percentage of EU citizens who seldom or never found false

[55] For instance: www.facebook.com/communitystandards/; https://help.twitter.com/en/rules-and-policies/twitter-rules

[56] https://ec.europa.eu/digital-single-market/en/digital-services-act-package

[57] (European Commission, 2018c); (European Commission, 2020d)

information increased 2 points, up to 19 % in 2020. Finally, the percentage of those who did not know if they came across false news or information increased 6 points, up to 9 % in 2020. The reduction of awareness is more worrying when considering specific population groups who are more vulnerable to disinformation, such as elderly people. In 2018, 61 % of people aged 55 or over declared having found false news or information at least once a week. In 2020, this percentage fell 14 points to 47 %.

The decrease in the levels of awareness about disinformation amongst European citizens shows the urgent need for public policies aimed at reverting this trend. Moreover, citizens themselves consider public intervention as the best way to raise awareness. 46 % of respondents to the Special Eurobarometer on the impact of digitalisation on their daily lives consider that public authorities should help citizens to better identify disinformation, with this being the most frequently mentioned public policy.

5.5. Current mechanisms of information sharing and coordination are proving insufficient

In recent years, the EU has developed a wide network of units, teams, agencies and other advisory bodies aimed at tackling the complex phenomenon of hybrid threats and one of its main components, disinformation. Additionally, Member States have also created specific units to combat hybrid threats at the national level involving different institutions (presidential cabinet, ministries of home affairs, foreign affairs, defence, etc.) and with diverse responsibilities (monitorisation, detection, attribution, response, etc.). The private sector is also collaborating through observatories, fact-checking networks and think tanks.

Notwithstanding EU efforts to create a comprehensive architecture to deal with hybrid threats, a better coordinated response is still lacking (Fiott, D. & Parkes, R., 2019). Although disinformation and cybersecurity are closely related, they are usually addressed in an isolated manner (Scheidt, M., 2019). Information sharing is also crucial to better address hybrid threats. However, sharing sensitive information between EU bodies, agencies and Member States remains difficult (Fiott, D. & Parkes, R., 2019). It is, therefore, necessary to design and implement new mechanisms of coordination and information sharing that allow hybrid threats to be countered in an effective and timely manner. Such mechanisms should consider the role of private agents, which must also act in coordination with public authorities.

5.6. The EU is falling behind its main competitors (the US and China) in the development of key digital technologies to tackle hybrid threats

The EU's technological dependence on foreign providers, mainly the US and China (Ortega, A., 2020), regarding sensitive areas like cyber-intelligence, cybersecurity, 5G infrastructure, and artificial intelligence can make it difficult to counter hybrid threats while respecting EU values and principles (right to the protection of personal data, rule of law, democracy, respect for individual freedoms, etc.). It also entails the risk of leaving very sensitive information in foreign hands, which could be misused against the EU's interests. Both reasons, along with others of a strategic and economic nature, make it necessary to lay the foundations and support the development of a robust European industry in key technological areas. As the President of the European Commission stated in her political guidelines for the next term, 'it may be too late to replicate hyperscalers, but it is not too late to achieve technological sovereignty in some critical technology areas' (von der Leyen, U., 2019, p. 13). Fortunately, critical technology areas where the EU can still contest the leadership of its competitors coincide with those that can contribute most to the fight against hybrid threats: artificial intelligence, blockchain and 5G.

5.7. Narratives of EU institutions and Member States try to debunk disinformation in retrospect

One of the main components of hybrid threats from the communication perspective is disinformation campaigns. They try to mislead citizens about current events by mixing false information with distorted interpretations of that reality. One of the most recently examples were the false accusations that to 5G networks are responsible for spreading the Covid-19 virus. Disinformation is quickly spread through digital platforms with the aim of amplifying their impact. According to a 2017 estimation, citizens in advanced countries might be consuming more false than true information by 2022 (Panetta, K., 2017).

The agents involved in the fight against disinformation normally adopt a reactive approach, trying to debunk false information once it has already been published and spread (Peter, M. et al., 2019). Thus, attackers usually take the lead and the victims (EU institutions and Member States) concentrate their efforts on refuting disinformation *ex post* and then deal with its effects. It is, therefore, necessary to adopt more proactive approaches to combatting disinformation, by leveraging strategic communications to anticipate the malicious actions of promoters of hybrid threats or, at least, limit their effects.

6. Policy options

The EU is currently undertaking diverse legislative amendments and policy actions to fight hybrid threats more effectively. It is worth mentioning the so called '*Digital Services Act Package*' (European Commission, 2020f), which intends to reform the legal framework for digital services to boost the European digital economy. It also includes proposals to unify responses and actions across the EU against false content and disinformation spread through online platforms. In light of the recent Covid-19 crisis, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy have launched a communication summarising the work done so far by the EU to combat disinformation around the pandemic (European Commission and the High Representative, 2020). The communication also includes the new actions that the EU should carry out to improve its response against disinformation. Finally, the EU Action Plan on Human Rights and Democracy 2020-2024 intends to reinforce the role of the EU as a global leader in promoting human rights and democracy across the world (European Commission and the High Representative, 2020a). The policy options proposed are aligned with these initiatives and provide a comprehensive framework to guide policymakers' action to better address hybrid threats affecting the EU and its Member States.

6.1. Assessment criteria

Policy options are grouped based on the challenges they seek to address, described in Chapter 5. They are analysed and assessed according to the following assessment criteria:

- Costs and benefits: whether the benefits obtained from the policy outweigh the costs and whether the policy is affordable for both public and private agents.
- Feasibility: whether the policy can be easily implemented, and it is likely to be supported by diverse stakeholders (politicians, civil society, economic sector) at both EU and national levels.
- Effectiveness: whether the policy is expected to achieve its goals.
- Sustainability: whether the policy can be maintained from an economic and political perspective until it achieves its objectives.
- Risks and future uncertainties: whether there are risks or uncertainties that can hinder the impact of the policy or create negative externalities.
- Coherence with EU objectives: whether the policy is aligned with the EU's vision and values.
- Potential ethical, social or regulatory impacts: whether the policy might have unexpected (or unwanted) ethical, social and regulatory impacts that may affect its effective completion.

The different policy options are assessed against each of these criteria by using a three-level scale: low if the policy does not adequately meet the criteria, high if the policy is likely to meet the criteria, and medium if the policy is somewhere in between. Table 9 summarises all proposed policy options.

Table 9: Summary of policy options

Policies related to regulation against hybrid threats
• Development of the European Strategy against Hybrid Threats, Disinformation and Foreign Interference (EU-HTDFI Strategy) • Regulation of risk analysis for hybrid threats • Improvement and harmonisation of the European legal framework against hybrid threats, disinformation and foreign interference • Adaptation of a sanction regime against promoters of hybrid threats, disinformation and foreign interference • Update of the interpretation made by the Cybercrime Convention Committee (T-CY) regarding interference in electoral processes • Improvement of regulation of artificial intelligence to address hybrid threats, disinformation and foreign interference
Policies related to attribution of hybrid threats
• Increasing economic resources allocated to the attribution of threats • Increasing economic resources allocated to the detection of disinformation
Policies related to the role of social media platforms in the fight against hybrid threats
• Making the Code of Practice on Disinformation mandatory, and adding periodic external audits
Policies aimed at raising awareness about hybrid threats
• Incorporation of critical information analysis competencies in school curriculums • Introduction of teacher training and ongoing development of educational resources and content • Introduction of policy-maker training • Introduction of digital literacy programmes for people with low digital competency • Promotion of citizen guides to detecting disinformation
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 • Intensified cooperation between the EU and NATO • Development of training exercises on countering hybrid threats involving all stakeholders • Increased operational intelligence capability at the EU level • Development of the European Cybersurveillance Tool (ECT) • Increased public-private collaboration
Policies related to the digital technology gap between the EU and its competitors
• Increased R&D investment and financial support for start-ups, and scaling 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 against hybrid threats
• Allowing public authorities to exceptionally intervene in digital services to counteract hybrid threats • Improving law enforcement in 5G networks
Policies aimed at defining proactive approaches to dealing with hybrid threats
• Strengthening the EU's vision and values outside the EU borders • Supporting free journalism against disinformation • Mandatory creation of StratCom units at the highest level in EU countries and institutions • Creation of an EU news agency to ensure veracity of information • Improvement of diplomatic relations with countries considered strategic challenges

Source: own elaboration

6.2. Policies related to regulation against hybrid threats

6.2.1. Development of the European Strategy against Hybrid Threats, Disinformation and Foreign Interference (EU-HTDFI Strategy)

The EU, aware of the dangerousness of hybrid actions and disinformation campaigns, has been working on different policy actions aimed at combating such threats: an action plan against disinformation, joint framework on countering hybrid threats, communication for tackling online disinformation, communication for increasing resilience and bolstering capabilities to address hybrid threats, communication for a strategic approach to resilience in the EU's external action, etc. These initiatives have been focused on implementing of practical measures such as the creation of the Hybrid Fusion Cell, the Hybrid CoE and the Rapid Alert System, the establishment of the StratCom Task Forces, the definition of the Code of Practice on Disinformation, etc. However, there has not been regulatory proposals (regulations, directives, etc.) to address this issue. In the fight against hybrid threats, the EU should follow the roadmap undertaken in the field of cybersecurity, where a cybersecurity strategy was firstly defined as the basis for the subsequent legal framework (NIS Directive, Cybersecurity Act, etc.), which allowed harmonisation of the legal response to cybersecurity issues in all Member States.

In order to define a coherent legal framework to allow Member States to tackle hybrid threats in a coordinated and harmonised way, the prior development of a European Strategy against Hybrid Threats, Disinformation and Foreign Interference (EU-HTDFI Strategy), which would act as the regulatory basis for the further implementation of specific legal instruments, would be advisable. The strategy would also serve to clarify all the work already done by the EU to counter hybrid threats, to evaluate the results and to define new practical tools when necessary.

Table 10: Assessment matrix for the policy option 'Development of the European Strategy against Hybrid Threats, Disinformation and Foreign Interference (EU-HTDFI Strategy)'

Criteria	Adequacy	Argument
Costs and benefits	High	The cost of enacting the European Strategy against Hybrid Threats, Disinformation and Foreign Interference (EU-HTDFI Strategy) would be very low. On the other hand, the benefits derived from its implementation would be very high because the Strategy would precisely delimit the future legal scope of EU operations against hybrid threats, disinformation and foreign interference.
Feasibility	Medium	The adoption of a strategic regulation as proposed would require a strong and unwavering commitment from all Member States.
Effectiveness	High	The effectiveness of the measure would be presumably be very high; not only because of the effectiveness of the Strategy itself, but also because it would be the basis for the enactment of the entire subsequent regulatory framework.
Sustainability	High	There would be no obstacles (economic or political) to maintaining the proposed Strategy in the future.
Risks and uncertainties	High	The risks and uncertainties of adopting a strategy such as the one proposed would be low, except for those inconveniences that might arise from those parties interested in maintaining the current *status quo*.
Coherence with EU objectives	High	The proposed strategy would be consistent with previous EU initiatives and could act as a driver for further actions.
Potential ethical, social and regulatory impacts	Medium	Given the absence of such a strategy in the current European legal system, it is to be expected that the impact would be appreciable from a social and regulatory point of view.

6.2.2. Regulation of risk analysis for hybrid threats

Risk assessments to identify vulnerabilities (social, economic, technical, etc.) should be one of the priority tasks addressed when dealing with hybrid threats at both the EU and the Member States levels. Knowing the risk to which society's essential assets are exposed is crucial in order to manage them. The need to use risk analysis mechanisms has already been highlighted in many European regulations such as the GDPR, the eIDAS Regulation, the NIS Directive, etc.

The risk analysis for hybrid threats, and especially for disinformation campaigns, should consider the following elements:

- Assets: the valuable components to be protected (confidence in the democratic political system and its institutions, social cohesion, independence and sovereignty of own decisions, maintenance of economic order, etc.).
- Threats: circumstances that may affect the assets, causing damage (caused by the EU and its Member States' own vulnerabilities).
- Safeguards (or countermeasures): protection measures deployed to eliminate or reduce the damage of threats.

In order to be effective, conducting risk analysis to counteract hybrid threats and disinformation should be a permanent activity (continuous monitoring) and should be legally regulated at the EU level and in

each Member State. Furthermore, taking advantage of the legal regulation of risk analysis, a common Risk Analysis Tool could be developed in relation to hybrid threats, disinformation and foreign interference.

Table 11: Assessment matrix for the policy option 'Regulation of risk analysis for hybrid threats'

Criteria	Adequacy	Argument
Costs and benefits	High	The costs of planning and implementing (on an ongoing basis - continuous monitoring) risk analysis for hybrid threats would be very low in relation to the expected benefits of its implementation, which will allow the threats that pose a greater risk as well as the probability of their occurrence to be identified.
Feasibility	High	There would be no significant drawbacks to implementing such a measure.
Effectiveness	High	If it is developed in a rigorous way, and in a permanent way, the effectiveness of the measure in reaching the indicated objectives would be very high.
Sustainability	High	There are no significant drawbacks that would limit the sustainability of the measure.
Risks and uncertainties	High	Conducting risk analysis for hybrid threats would not pose any significant risk to the EU, beyond the need to keep some results of the risk analysis confidential.
Coherence with EU objectives	High	Maintaining continuous monitoring of the risks posed by hybrid threats to the EU is perfectly aligned with the objectives of the EU and its *action plan against disinformation*.
Potential ethical, social and regulatory impacts	Medium	Regarding ethical and social issues, continuous monitoring of risks should respect privacy and personal data protection. The greatest impact could come from the need to adopt complementary legal measures, by virtue of the results of such a risk analysis.

6.2.3. Improvement and harmonisation of the European legal framework against hybrid threats, disinformation and foreign interference

Combating the communications components of hybrid threats, especially when they come from foreign states, requires an appropriate legal framework. Being aware of this necessity, certain EU Member States (such as France and Germany)[58] have incorporated norms into their own legal systems to regulate the response to disinformation or foreign interference aimed at undermining confidence in national institutions and endangering the quality of democratic processes. The European Commission also addressed this issue in its package of measures to protect the 2019 European elections (European Commission, 2018g). However, a harmonised legal framework to fight disinformation at the EU level is still lacking. It should be drafted, discussed and approved within the EU institutions (in the legal form of a directive or a regulation), to be applied to digital sources, platforms and social networks, with the following essential objectives:

[58] In France: Decree no. 2015-125 of 5 February 2015 or the new laws approved by the National Assembly in November 2018 (*Loi organique n° 2018-1201 (et 2018-1202) du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*). In Germany: Act to improve Enforcement of the Law in Social Networks (*Netzwerkdurchsetzungsgesetz* or NetzDG), entered into force in January 2018.

- Clarifying the liability regime for online intermediaries regarding false content.
- Ensuring the commitment of digital social sources and online content distribution platforms (social networks, video platforms, etc.) in the fight against disinformation, making them responsible for the removal of illegal, harmful or false content.
- Unifying notice-and-action procedures that allow users to report the existence of possible illegal, harmful or false content so that the platforms can quickly investigate the reported content and, if necessary, remove it.
- Imposing transparency obligations for online platforms about their activity against disinformation.
- Allowing Member States to suspend foreign-controlled digital sources or platforms that spread false news, considering such decisions as compatible with EU rules, particularly the Audiovisual Media Services Directive.

In addition, this new regulatory framework should pay particular attention to preventing foreign influence in electoral periods by means of:

- Prohibiting foreign funds to pay advertising campaigns trying to influence elections or obliging online platforms to maintain and publish a registry of partisan advertising before and during the electoral period.
- Clarifying offences related to publishing of false statements aimed at interfering in election results.

This new regulation should also consider the development of indicators of reliability and transparency of information sources, as well as allowing the research community to access relevant public databases in order to detect and analyse disinformation campaigns more rigorously and effectively.

Table 12: Assessment matrix for the policy option 'Improvement and harmonisation of the European legal framework against hybrid threats, disinformation and foreign interference'

Criteria	Adequacy	Argument
Costs and benefits	High	The law has always served as a strategic enabler and constraint in international relations (Sari, A., 2020). The proposed policy option, as a direct consequence of the enactment of the European Strategy against Hybrid Threats, Disinformation and Foreign Interference (EU-HTDFI Strategy) which has been outlined above, will regulate those behaviour of digital sources and online platforms (internal and external to the EU) and also others that should be subject to legal reproach, always maintaining the maximum respect for the rights and freedoms of EU citizens. This regulation would imply extra costs for online platforms operating in the EU, but the benefits for the society as a whole would be much higher.
Feasibility	Low	A legislative package such as the one proposed involves previous actions at different levels (political, economic and social) which, in the end, will have to be discussed in the European Parliament. All this involves certain difficulties. At present, the position of Member State governments is divided on the need to adopt specific regulations to tackle disinformation campaigns and foreign interference. Finally, if legislative proposals are adopted in the form of a European directive, it will also be necessary to consider the disadvantages arising from their transposition into Member States' legal systems.

Effectiveness	High	The legal measures, formally approved by the European Parliament, constitute one of the greatest guarantees for combating hybrid threats.
Sustainability	Medium	Like any Europe-wide regulatory package, this proposal will require additional and ongoing efforts to ensure its sustainability over time.
Risks and uncertainties	Low	As this is an unprecedented regulatory package at the EU level, there may be risks and uncertainties at all stages of its development: prior analysis, drafting, adoption and entry into force of the draft legislation. There are also other related legislative amendments in course (like the Digital Services Act Package) which could collide with this proposal.
Coherence with EU objectives	High	The development of a legislative package such as the one proposed is in line with the European Strategy against Hybrid Threats, Disinformation and Foreign Interference (EU-HTDFI Strategy) mentioned above and with the EU action plan against disinformation.
Potential ethical, social and regulatory impacts	Low	Since this is the development and approval of a policy package, the regulatory impact would presumably be high.

6.2.4. Adaptation of a sanction regime against promoters of hybrid threats, disinformation and foreign interference

As the European Council states, 'restrictive measures or sanctions are an essential tool of the EU's Common Foreign and Security Policy (CFSP). They are used by the EU as part of an integrated and comprehensive policy approach, involving political dialogue, complementary efforts and the use of other instruments at its disposal' (European Council, 2020b). Sanctions have been widely used as a foreign policy instrument at both international (the UN) and regional (the EU) levels in recent years. Whereas previously the sanctioning regimes were comprehensive, and thus affected the civilian population, now they tend to be more accurate (smart sanctions), targeting specific individuals or entities (Happold, M., 2016).

Strict and effective enforcement of the regulatory package outlined in the previous policy option would require the imposition of sanctions on actors who fail to comply with its provisions, i.e. those who encourage, promote or carry out hybrid actions, disinformation campaigns or illegally interfere with the normal functioning of the EU institutions or Member States. Hybrid threats and their components should, therefore, be considered as a cause that could lead to a sanction. The regulatory package developed in the previous policy option should contain a specific chapter dedicated to detailing such sanctions.

Table 13: Assessment matrix for the policy option 'Adaptation of the legal framework for sanctions against promoters of hybrid threats, disinformation and foreign interference'

Criteria	Adequacy	Argument
Costs and benefits	High	The regulatory package outlined in the previous policy option should be complemented with a clear proposal of sanctions for those (inside or outside the EU) who do not comply with this regulation. This policy would not entail any cost to the EU or its Member States.

Feasibility	Medium	The determination of sanctions is always a thorny issue with many facets, which hampers their development and adoption, especially when, as in the present case, there may be difficulties in the attribution of authorship. Some countries would be reluctant to support sanctions to counter hybrid threats.
Effectiveness	High	The imposition of rigorous and proportionate sanctions for promoting hybrid threats would undoubtedly contribute to reducing their presence and impact.
Sustainability	Medium	Determining which conduct deserves legal reproach should be an issue agreed on by all Member States. It would also need to be periodically updated, which would entail the continuous effort of assessing the results of the sanctions regime.
Risks and uncertainties	Medium	All proposals involving the establishment of a sanctioning regime are uncertain as to the appropriateness of the sanction, its proportionality, its enforcement and its ultimate effectiveness.
Coherence with EU objectives	Medium	Only in certain cases has the EU opted for sanctions against third states, companies or even individuals, so the adoption of such a measure, although not far removed from EU objectives, should be considered an exception.
Potential ethical, social and regulatory impacts	Medium	The regulation of a sanctioning regime always has a significant impact on the applicable legal regime, as well as on the society.

6.2.5. Update the interpretation made by the Cybercrime Convention Committee (T-CY) regarding interference in electoral processes

The Cybercrime Convention Committee (T-CY) issued the Guidance Note #9 '*Aspects of election interference by means of computer systems covered by the Budapest Convention*' with the aim of addressing 'how articles of the Convention may apply to aspects of election interference by means of computer systems' (Cybercrime Convention Committee (T-CY), 2019).

The T-CY stated that the substantive crimes in the Convention may be carried out to facilitate, participate in or prepare acts of election interference and the procedural and mutual legal assistance tools in the Convention may be used to investigate election interference, its facilitation, participation in it, or preparatory acts.

The T-CY pointed out the following types of crime that interfere in electoral processes, using information systems:

- Illegal access (art. 2): A computer system may be illegally accessed.
- Illegal interception (art. 3): Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted.
- Data interference (art. 4): Computer data may be damaged, deleted, deteriorated, altered, or suppressed.
- System interference (art. 5): The functioning of computer systems used in elections or campaigns may be hindered for the purpose of interference.
- Misuse of devices (art. 6): The sale, procurement for use, import, distribution or other acts making computer passwords, access codes, or similar data available.

- Computer-related forgery (art. 7): Computer data (for example the data used in voter databases) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.

All the previous assumptions of interference are based on damage to the information systems used in electoral processes, negatively affecting the dimensions of security: **availability**, **confidentiality** and **integrity**.

However, disinformation campaigns and foreign interference also impact a new dimension of security: the **truthfulness** of the information poured into digital sources, on-line platforms or social networks.

Therefore, it is advisable to create a new T-CY activity to study the incorporation of the lack of ***truthfulness*** as an element that, in certain cases, can constitute a crime.

Table 14: Assessment matrix for the policy option 'Update the interpretation made by the Cybercrime Convention Committee (T-CY) regarding interference in electoral processes'

Criteria	Adequacy	Argument
Costs and benefits	High	The inclusion of the requirement to maintain the ***truthfulness*** of the information in digital sources, in accordance with the Budapest Convention, would make it possible to better address electoral interference. This policy would not entail additional costs.
Feasibility	Low	Updating of the interpretation of the postulates of the Budapest Convention requires prior analysis by all signatory parties, which makes its adoption difficult, without prejudice to the transfer of the new postulates to the regulations of the Member States and their judicial administrations.
Effectiveness	High	If an agreement was reached on the interpretation of lack of truthfulness as a crime, the effectiveness of the measure would be very high, because it would allow for the formal prosecution of certain behaviours that are currently interfering in elections in Europe.
Sustainability	High	Once the agreement is reached, the sustainability of the agreement would be high.
Risks and uncertainties	High	Once the agreement is reached, the risks and uncertainties would be like any other risks arising from the adoption of new regulations or legal interpretations.
Coherence with EU objectives	High	As the EU is the promoter of the Budapest Convention, it has the greatest interest in keeping it up-to-date by considering new behaviours that could be considered crimes.
Potential ethical, social and regulatory impacts	Low	The impact, in terms of criminal law, will be very high, as the measure could introduce new types of crimes.

6.2.6. Improving regulation of artificial intelligence to address hybrid threats, disinformation and foreign interference

Artificial intelligence plays a double role in the realm of hybrid threats. It can be used for criminal purposes to deceive people by creating and spreading false information, and it can also contribute to the fight against disinformation, especially in key areas such as prevention, detection and attribution.

Delivering on its AI strategy adopted in April 2018 (European Commission, 2018d), in December 2018 the Commission presented a coordinated plan, prepared together with the Member States, to foster the development and use of AI in Europe (European Commission, 2018i). This plan comprised some 70 joint actions for boosting AI development and increasing market uptake in Europe. One of the key areas stressed by the Commission was the use of AI solutions for improving public services and, in general, the performance of EU and Member States institutions. Within this area, it is advisable to develop an adequate legal framework capable of regulating the use of IA by the public sector with the triple purpose of preventing, detecting and responding to hybrid threats, disinformation and external interference.

Table 15: Assessment matrix for the policy option 'Improve regulation of artificial intelligence to address hybrid threats, disinformation and foreign interference"

Criteria	Adequacy	Argument
Costs and benefits	High	AI will continue to grow and develop in the coming years, and the benefits derived from its adoption as a support tool for countering hybrid threats through strategic communications would gradually increase without raising significant costs.
Feasibility	High	The EU is already working on AI regulation. This would involve regulating its use for one particular aspect: the fight against hybrid threats, disinformation and foreign interference.
Effectiveness	High	The possibilities of AI are enormous and are in full development. Therefore, it seems reasonable to expect this measure to be highly effective.
Sustainability	High	Once the corresponding regulations are enacted, the sustainability of the measure is high, beyond the necessary updating required by technological evolution.
Risks and uncertainties	Medium	Any activity that implies the use of technologies, products or services based on AI poses risks and uncertainties in its development, due to it being a disruptive technology,
Coherence with EU objectives	High	The EU has embarked on a determined path towards the use and regulation of AI, so the measure proposed is perfectly consistent with EU objectives.
Potential ethical, social and regulatory impacts	Medium	As mentioned above, any activity involving the use of AI-based technologies, products or services poses risks and uncertainties that should be mitigated by the proposed regulation.

6.3. Polices related to attribution of hybrid threats

6.3.1. Increasing economic resources allocated to the attribution of threats

Identifying the source of hybrid threats requires adequate resources, both human and technical.

Hybrid threats evolve rapidly alongside new technologies, so investment in resources must be constant. The technological tools available to agencies investigating threat authorship need to be kept up-to-date. Human resources (digital forensic researchers, journalists, psychologists, sociologists, lawyers, law enforcement corps, intelligence analysts, etc.), properly trained and with the right skills, must also be suitable for the task of research and analysis.

There is no data on Europe's actual spending on investigating hybrid threats and identifying perpetrators, but if current investment in cyber security, one of the most important frameworks for combating these threats, is considered, it is clear that there is room for improvement. The European Court of Auditors, in a briefing paper named *Challenges to Effective EU Cybersecurity Policy* states the following regarding cybersecurity spending in Europe: 'Spending in the EU has been low by comparison, fragmented and often not backed by concerted government-led programmes. Figures are hard to come by, but EU public spending on cybersecurity is estimated to range between €1-€2 billion per year. Some Member States' spending as a percentage of GDP is one-tenth of US levels, or even lower' (European Court of Auditors, 2019).

Resources for the attribution of threats should be made available at both the EU and national levels, and investment from the private sector is also required.

In addition to increasing economic resources, the EU could also work on the definition of a Model for the Authorship of Hybrid Threats and Disinformation, aimed at achieving a common European position on attributing and sanctioning of hybrid threats, disinformation and foreign interference.

Table 16: Assessment matrix for the policy option 'Increasing economic resources allocated to the attribution of threats'

Criteria	Adequacy	Argument
Costs and benefits	Medium	Increasing technological sophistication would require technical and human resources. The cost of keeping the available resources properly trained and updated can be high.
Feasibility	Low	The current health-related economic crisis in Europe may make it difficult to allocate sufficient resources for the identification of perpetrators. Rising expenditure might be particularly complicated for those Members States that have suffered a high impact due to the Covid-19 crisis.
Effectiveness	High	Identifying the perpetrator would allow responsibilities to be clarified and sanctions to be applied, as well as raising public awareness about the real objectives behind the attacks.
Sustainability	Medium	Sustainability of investments will depend on the availability of funds and the political commitment of governments. Solutions would need to be updated very regularly and human supervision is still necessary.
Risks and uncertainties	High	No particular risks have been identified.
Coherence with EU objectives	High	Identifying the perpetrator is the first step towards accountability and transparency, therefore it is totally in line with the EU principles and policies.
Potential ethical, social and regulatory impacts	Medium	No ethical, social or regulatory impacts have been identified as resulting from increasing economic resources allocated to the attribution of threats. The European agreement on the attribution of authorship of hybrid threats, disinformation and foreign interference would have a significant impact on the implementation of regulatory measures that may subsequently be developed.

6.3.2. Increasing economic resources allocated to the detection of disinformation

A 2019 study from the company CHEQ and the University of Baltimore estimated the cost of disinformation at US$78 000 million annually. This amount includes losses in stock market value, costs derived from health misinformation, reputation management and brand equity costs, financial misinformation (only in the US) and election costs of fake political advertisements. Furthermore, it only refers to the direct losses and opportunity costs imposed on society by disinformation (Cavazos, R., 2019).

In contrast, in 2019 the European External Action Service strategic communication budget reached €5 million (Scheidt, M., 2019).

Investments need to be increased at the national level, but also at the EU level, both from public authorities and the private sector.

This investment should include, but not be limited to:

- Development and support of fact checkers.
- Research and development of new tools for identifying and tracking disinformation, including support for start-ups.
- Skill development for key agents and public servants.

Efforts should be made in two directions: disproving disinformation, and identifying disinformation sources and means of transmission to label the content and warn users of its dubious origin.

While exposing disinformation through fact checkers can be a useful tool to stop the spread of disinformation and therefore limit the damage it causes, the impact of denials is often much less than that of the false news itself. Therefore, advisory labels for suspicious content coming from dubious sources could be helpful in minimising the impact of disinformation in a more effective way than retroactive measures.

Table 17: Assessment matrix for the policy option 'Increasing economic resources allocated to the detection of disinformation"

Criteria	Adequacy	Argument
Costs and benefits	Medium	The costs of identifying and tracking disinformation can be very high, as media, channels and technologies change and evolve very quickly. Also, the benefits of identifying disinformation may be limited. While stopping its spread is very important and can have a high impact, exposing and disproving disinformation often does not have the same impact as the disinformation itself, so the cost-benefit of doing so may be limited.
Feasibility	Low	The current health-related economic crisis in Europe may make it difficult to allocate sufficient resources to the detection of disinformation. Rising expenditure might be particularly complicated for those Member States that have suffered a high impact due to the Covid-19 crisis.
Effectiveness	Medium	Specific news denials may be ineffective. However, identifying sources of disinformation and labelling dubious information can be very effective tools in curbing disinformation.

Sustainability	Medium	Sustainability of investments will depend on the availability of funds and the political commitment of governments. Solutions will need to be updated very regularly and human supervision is required to ensure respect for fundamental rights.
Risks and uncertainties	High	No particular risks have been identified.
Coherence with EU objectives	High	Disinformation is a major challenge for democratic values and systems and tackling its spread through detection is a priority for the EU.
Potential ethical, social and regulatory impacts	Medium	It may imply the need for legal changes, as well as changes to the terms and conditions of use of some services. Potential conflicts with data protection regulations and limitations of freedom of speech may also arise.

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

6.4.1. Making the Code of Practice on Disinformation mandatory, and adding periodic external audits

At present, European regulation (particularly the eCommerce Directive) guarantees digital platforms an exemption of responsibility as providers of an intermediary service, while ensuring their collaboration with authorities on fighting against illegal content. However, the special nature of disinformation, which may be legal but potentially harmful, requires the issue to be addressed through a different approach. This debate is taking place in Europe with the current discussions over the new Digital Service Act, but also in the USA, where public controversy around labelled and removed publications on Twitter led the former Trump Administration to start a debate on the legal consideration of digital platforms and their responsibilities regarding the content (The White House, 2020). In Europe, and regardless of what is finally established by the Digital Services Act, the Code of Practice on Disinformation can be a powerful tool in fighting disinformation on social media platforms.

The code was an important step in the fight against disinformation. Through the code, signatories committed to implementing self-regulatory measures to counter false information. The code includes several commitments considered of critical importance in countering flows of disinformation on social media platforms:

- Control of the use of bots that allows massive diffusion of disinformation. This includes identity theft through fake accounts.
- Transparency of algorithms that decide which news or advertising to display to users.
- Different strategies to deal with dubious content by means of alerts or labels.

In order to leverage the full potential of the code, signing it could be a precondition for operating in the EU for digital platforms and related companies. At the same time, to improve the effectiveness of the code, independent external audits and sanctions for non-compliance should be applied. Such measures (mandatory adhesion to the code and independent audits on compliance with commitments) were mentioned in the conclusions of the Council of the European Union at the end of 2019 (European Council, 2019b).

Regarding implementation of this policy option, special attention should be paid to the upcoming audit of the European Court of Auditors of the Action Plan against Disinformation, which will assess the results of implementing the Code (European Court of Auditors, 2020).

Table 18: Assessment matrix for the policy option 'Making the Code of Practice on Disinformation mandatory, and adding annual external audits'

Criteria	Adequacy	Argument
Costs and benefits	Medium	For potential new signatories, the mandatory character of the code would imply extra effort and investment in order to comply with commitments. But the possibility of operating in the EU is probably attractive enough to make the necessary investment.
Feasibility	High	The code has already been signed by the main digital companies and social media platforms, and the third-party revision of the implementation reports is currently a possibility. The policy option recommended would not pose great changes for current or new signatories, while it could mean an important boost to the implementation of the code. The main social media platforms are part of multinational companies, thus the relevance of applying changes to the code remain at the EU level.
Effectiveness	High	The simple fact of signing the code supposes a qualitative important step in countering disinformation on social media platforms. The independent audit ensures that efforts to comply with commitments are real.
Sustainability	High	For both the EU and multinational companies in charge of digital platforms, actions to comply with the code should not involve a great economic cost. Even though the Code of Practice seems to be a permanent measure. For smaller companies, however, the cost could imply a greater economic effort.
Risks and uncertainties	Medium	New social media platforms could decide to not start operating in Europe due to the mandatory adhesion to the Code of Practice.
Coherence with EU objectives	High	The Council of the European Union has already suggested these specific policies.
Potential ethical, social and regulatory impacts	Medium	Sanctions should be regulated adequately. Limitations or actions contrary to popular social networks can generate social discomfort.

6.5. Policies aimed at raising awareness about hybrid threats

6.5.1. Incorporation of critical information analysis competencies in school curriculums

The objective of including competencies in critical analysis of information in school curriculums is to provide citizens with tools to identify disinformation and develop critical thinking skills and media literacy from a young age. Today, critical thinking requires considering the relevance of the digital environment, and the values it should encompasses: participation, transparency and accountability.

Developing critical thinking skills to counter disinformation has proven to be effective by helping people identify this type of information and reduce its impact on personal beliefs and values. For example, the non-governmental organisation IREX trained 15 000 people to identify disinformation and recognise manipulation and hate speech. Subsequent evaluation of the programme confirmed a 24 % increase in participants' ability to distinguish trustworthy news from false news, a 22 % increase in information cross-checking, and a 26 % increase in participants' confidence (Buluc, R., 2018).

Critical thinking is one of the competencies included in the Council Recommendation of 22 May 2018 on key competencies for lifelong learning (European Council, 2018b, p. 9). However, it has not yet been incorporated into the formal education curriculum of many of EU countries.

Finland was the first European country to implement a nationwide initiative against disinformation in 2014. In 2016, right after the US election campaign, the critical thinking curriculum was revised to prioritise skills to identify disinformation. As a result, according to the Media Literacy Index from the European Policies Initiative (EuPI) at the Open Society Institute (Sofia), Finland is ranked top of the 35 countries, and is 'considered the best equipped to withstand the impact of disinformation due to the quality of education, free media and high trust among people' (Open Society Institute Sofia, 2019).

Critical thinking and information analysis competencies should include the development of the skills needed to evaluate sources, use text responsibly, better understand the impact of disinformation and identify one's own biases and ideology.

Table 19: Assessment matrix for the policy option 'Incorporation of critical information analysis competencies in school curriculums'

Criteria	Adequacy	Argument
Costs and benefits	High	The benefits of developing critical thinking and digital skills amongst children and young people are very high, as it is the most effective way to build a resilient society for the future. Costs may include reviewing school curricula and, in some cases, developing educational materials, but this can be done at a very low cost through open educational resources at the European level.
Feasibility	Medium	Education is a national competence and therefore such policies are implemented at the national or regional levels. The political feasibility of the measure may be constrained in some countries due to ideological struggles, particularly in decentralised countries and places where disinformation is highly politicised.
Effectiveness	High	Education and awareness at an early age is probably one of the most effective policies in terms of strengthening the resilience of society.
Sustainability	High	The education of young people is a medium- and long-term policy that guarantees the sustainability of the action in the future, since it is not a one-off action, but one that has a sustained impact over time.
Risks and uncertainties	Medium	There is a risk of content being politicised in training of this nature. Additionally, educational policies require the participation of multiple stakeholders with varying interests and achieving compromises may be difficult.
Coherence with EU objectives	High	Awareness-raising and resilience building have been key policies for the EU in tackling the spread and impact of disinformation and ensuring European values and democratic systems are protected.

Potential ethical, social and regulatory impacts	Medium	High levels of politicisation of the topic in certain countries might cause social tensions.

6.5.2. Teacher training and ongoing development of educational resources and content

Teacher training is a prerequisite for the inclusion of critical thinking competencies in schools curriculums. Teachers must develop their own skills and understand the methodologies and tools in order to educate their pupils.

This training should be part of continuous on-the-job teacher training as the content needs to be regularly updated to keep up with technological developments and changes in attackers' strategies.

Table 20: Assessment matrix for the policy option 'Teacher training and ongoing development of educational resources and content'

Criteria	Adequacy	Argument
Costs and benefits	High	Teacher training is an essential prerequisite for the proper training of students. In-service teacher training could include this type of training at reduced costs thanks to new technologies.
Feasibility	Medium	Education is a national competence and therefore such policies are implemented at the national or regional levels. The political feasibility of the measure may be constrained in some countries due to ideological struggles, particularly in decentralised countries and places where disinformation is highly politicised.
Effectiveness	High	Effectiveness is very high, greater than that of communication campaigns. Moreover, it is essential for the correct training of the citizenship.
Sustainability	High	Educating young people is a medium- and long-term policy that guarantees the sustainability of the action in the future, since it is not a one-off action, but one that has a sustained impact over time. Teacher training is a prerequisite for training children.
Risks and uncertainties	Medium	There is a risk of content being politicised in training of this nature.
Coherence with EU objectives	High	Awareness-raising and resilience-building have been key policies for the EU in tackling the spread and impact of disinformation, and ensuring European values and democratic systems are protected.
Potential ethical, social and regulatory impacts	Medium	High levels of politicisation of the topic in certain countries might cause social tensions.

6.5.3. Policy-maker training

Legislators and policy-makers have a fundamental role, not only in the production of laws and public policies, but also as opinion leaders.

The participation of decision-makers in the dissemination of hoaxes is an important element of political destabilisation and polarisation of society, and therefore their role in raising awareness in society is very important.

Policy-makers must be champions in the fight against disinformation, and they must have the right skills and tools to do so.

Table 21: Assessment matrix for the policy option 'Policy-maker training'

Criteria	Adequacy	Argument
Costs and benefits	High	There are currently very low-cost training tools and methodologies with very low costs that make this policy very suitable due to its high benefit.
Feasibility	High	Training for policy-makers at all levels can be easily provided through online or face-to-face training conducted by their working institutions as part of their duties.
Effectiveness	High	Policy-makers have an impact both on policies and on public opinion. Making them aware of the importance of stopping disinformation and giving them the skills and tools to do so would have a very high impact.
Sustainability	High	Training needs to be updated and costs can be very limited thanks to online training methodologies. The impact will be sustained over time.
Risks and uncertainties	High	No particular risk has been identified.
Coherence with EU objectives	High	Better policy-making is highly coherent with EU objectives and values. Awareness-raising and resilience-building have been key policies for the EU in tackling the spread and impact of disinformation, and ensuring European values and democratic systems are protected.
Potential ethical, social and regulatory impacts	High	Policy-makers are expected to lead by example. Additionally, they have a responsibility towards citizens regarding the veracity of the information they manage in their decision-making processes. The impact of the information they manage is critical to the quality of regulations.

6.5.4. Digital literacy programmes for people with low digital competency

Strategic communication actions aimed at raising awareness amongst citizens have proven to be an effective way to tackle hybrid attacks in two domains:

1. Reducing the expansion of disinformation. When people acknowledge that information is false or misleading, the spread of disinformation can be stopped.
2. Limiting the damage of disinformation. Inflaming the feelings of the population at critical moments, increasing the polarisation of society, and destabilising democratic institutions by

attacking their legitimacy are some of the objectives of disinformation that can be prevented by building understanding and consciousness.

Understanding the impact of disinformation impacts and the aims behind it improves societal resilience. This requires not only communication campaigns, but also training in critical skills. In this sense, media literacy is a vital tool in fighting the proliferation of disinformation through online means. This fact has already been acknowledged by the EU, and the Commission has put initiatives into place to improve media literacy among the elderly, such as the Media Literacy Expert group (European Commission, 2019a) and the Preparatory Action 'Media Literacy for All' (European Commission, 2020a).

However, digital literacy is worsening. In 2017, the EU27 average of people with low overall digital skills between 55 and 74 years old was 28 %, while in 2019 this average rose to 34 % (Eurostat, 2020). The widening of this gap shows the need to increase efforts and investment.

Table 22: Assessment matrix for the policy option 'Digital literacy programmes for people with low digital competency'

Criteria	Adequacy	Argument
Costs and benefits	Medium	Digital literacy programmes aimed at reducing the digital skill gap exist around the EU, so programmes do not need to be created from scratch, only updated. However, the benefits are difficult to assess in the short term and the costs of massive programmes may be high.
Feasibility	Medium	Europe has funding mechanisms for training people, and digital literacy programmes are already in place in many EU countries. There are, however, differences between countries that authorities (national and regional) and sectorial associations should take into account, thus challenging the execution and follow-up of the policy.
Effectiveness	Medium	Effectiveness of these programmes is difficult to assess in the short term.
Sustainability	Medium	Digital literacy programmes aimed at reducing the digital skill gap are common in Europe and tend to be sustained over time. However, doing it on a large scale is costly.
Risks and uncertainties	High	No particular risks are identified.
Coherence with EU objectives	High	The EU is strongly committed to promoting digital skills and reducing the skills gap.
Potential ethical, social and regulatory impacts	High	No ethical, social or regulatory impacts have been identified.

6.5.5. Promoting citizen guides to detecting disinformation

The production of informative guides to help detect hoaxes and disinformation would increase awareness of these practices and provide citizens with tools to prevent their spread.

To be effective from the point of view of strategic communications, two elements are necessary. The first concerns their format and style. They must be sufficiently attractive and accessible to all citizens. The second concerns their dissemination, which must be massive in order to fulfil their objective.

Therefore, different versions adapted to different targets should be developed, especially taking into account age and educational level. Formats and distribution channels should be appropriate for this purpose.

Making these resources directly available through the main channels of dissemination of disinformation, such as social media or media outlets, would be desirable.

Table 23: Assessment matrix for the policy option 'Promoting citizen guides to detecting disinformation'

Criteria	Adequacy	Argument
Costs and benefits	High	The cost of producing the guides is low. Distribution can be done through collaboration with national, regional and local authorities, and with the private sector, in particular social media providers and the other stakeholders involved.
Feasibility	High	Feasibility is higher if guidelines are produced at the EU level and distributed locally and in collaboration with the private sector.
Effectiveness	High	Guidelines elaborated in the correct format (visual, intuitive, attractive) can have a very high impact in raising awareness amongst citizens. However, massive dissemination is essential for them to be effective.
Sustainability	Medium	Guides need to be constantly updated and their impact of its communication is difficult to sustain over time.
Risks and uncertainties	High	No particular risks are identified.
Coherence with EU objectives	High	Awareness-raising and resilience-building have been key policies for the EU in tackling the spread and impact of disinformation and ensuring European values and democratic systems are protected.
Potential ethical, social and regulatory impacts	High	No ethical, social or regulatory impacts have been identified.

6.6. Policies related to coordination and information-sharing between stakeholders

6.6.1. Creation of a coordination unit at the EU level to unify responses against hybrid threats

In recent years, the EU has developed diverse bodies to address hybrid threats from different perspectives: cybersecurity, information, crisis management, diplomacy, etc. (Scheidt, M., 2019). Some of these bodies also involve Member States. However, a specific unit that coordinates all efforts in the fight against hybrid threats is still lacking. This coordination unit would contribute to unifying responses and actions to counter hybrid threats that aim to destabilise any Member State or the EU as a whole. The coordination unit would allow better effectiveness of the measures adopted to mitigate and even prevent the effects of hybrid threats, as well as to send a clear message of firmness to the attackers. It should also undertake the creation of secure and rapid communication channels to inform stakeholders of the threats identified.

The coordination unit would also assume the responsibility of engaging the private sector and civil society to collaborate in the overall strategy to counter hybrid threats.

The coordination unit could be made up of representatives from all EU bodies currently involved in dealing with hybrid threats (European Commission, European Parliament, European Council, EEAS, ENISA, etc.), as well as Member States and representatives of critical companies from the private sector. However, to ensure its agility and effectiveness it should be managed by a reduced committee led by an experienced person who could come from the public or private sector: the EU Counter Hybrid Threat Coordinator (EU-CHTC).

The coordination unit's work should not be limited to occasional and isolated actions (such as responding to a specific crisis) but should be developed continuously over time.

Table 24: Assessment matrix for the policy option 'Creation of a coordination unit at the EU level to unify responses against hybrid threats'

Criteria	Adequacy	Argument
Costs and benefits	High	The existence of a coordination unit at the highest level would improve the EU's response to hybrid threats. Although such a unit should be provided with sufficient resources to function properly, the cost would be outweighed by the benefits that it could have for the whole EU.
Feasibility	Medium	Creation of the coordination unit would imply that departments and agencies at both the EU and Member State level should cede key parts of the strategy for countering hybrid threats to that unit.
Effectiveness	High	The coordination unit would allow the EU to demonstrate and exert unified action against hybrid threats, improving its response capabilities. It could also be used as a deterrence measure by showing attackers a firm determination to counter their threats.
Sustainability	High	The coordination unit should be maintained over time. However, by its nature, the structure should not be very large as it is not created to replace the work of other bodies and agencies but to coordinate their efforts.
Risks and uncertainties	Medium	Some EU countries could interpret the creation of the coordination unit as a loss of sovereignty regarding foreign affairs and the responses they can develop.
Coherence with EU objectives	High	The coordination unit is highly aligned with EU objectives, as it would allow reinforcement of the unity of EU action against hybrid threats. It would respect the principle of subsidiarity and only provide further coordination to enhance the effectiveness of responses.
Potential ethical, social and regulatory impacts	Medium	National regulations could make it difficult to share sensitive intelligence information, an essential asset in coordinating responses, with an EU body.

6.6.2. Creation of common response mechanisms at the EU level

The response to hybrid threats is mainly a national competence, and it is carried out almost entirely by Member States. Each country defines its own response measures and the strategies to address hybrid threats. The European Commission itself acknowledges this fact: 'Strengthening resilience to these

threats and bolstering capabilities are predominantly Member State responsibilities' (European Commission, 2018e). However, a common framework to harmonise national responses to hybrid threats would be advisable. It would allow hybrid threats to be addressed in a homogeneous way in any EU country. This kind of common framework would send a clear warning to attackers: all Member States are fully committed to the fight against hybrid threats, and attacks will receive the same response no matter where they occur. The common framework to address hybrid threats should encompass responses in the following fields:

- Creation of analogous criminal offences in all EU countries to combat hybrid threats.
- Definition of guidelines to develop common communication strategies at the national level.
- Coordination of diplomatic actions between Member States.
- Unification of sanction regimes against promoters of hybrid threats.

The EU could recommend (or even mandate) Member States to push forward in the adoption of common responses to hybrid threats.

Table 25: Assessment matrix for the policy option 'Creation of common response mechanisms at the EU level'

Criteria	Adequacy	Argument
Costs and benefits	High	The adoption of common response mechanisms by all Member States will benefit the EU as whole, demonstrating an image of unity in confronting hybrid threats. The implementation of responses at the national level could have a relevant cost. However, the benefits far outweigh the potential costs.
Feasibility	Low	The creation of common response mechanisms might be hampered by the diverse nature of the hybrid threats faced by each Member State. While some countries are addressing hybrid threats promoted by domestic actors, other countries are more exposed to foreign influence. Additionally, cultural, social and legal differences between EU countries would make it difficult to address all hybrid threats in a similar way.
Effectiveness	High	A common response by all EU countries would increase the effectiveness of the measures adopted against hybrid threats, regardless of which country was attacked.
Sustainability	High	A common set of response measures should be developed. Once such measures are defined, it would only be necessary to monitor them to ensure they meet their objectives, which could be done at a low cost.
Risks and uncertainties	Medium	Hybrid threats are not static. They evolve over time, becoming more sophisticated. There is a risk that reaching a common response framework between all Member States will take so long that it will become obsolete. The post-coronavirus geopolitical landscape could modify the current alliances between Member States and other countries traditionally considered hybrid threat sponsors (the best example could be China), posing new challenges to the creation of common responses to hybrid threats.

Coherence with EU objectives	High	This policy is aimed at providing a common European response to the phenomenon of hybrid threats, strengthening ties between Member States.
Potential ethical, social and regulatory impacts	Medium	The production of common responses to hybrid threats do not raise ethical and social issues, as long as such responses respect civil rights and European values. At the regulatory level, this policy option could have a great impact. Unifying legal regimes in all Member States could be a very highly complex task and could take a long time.

6.6.3. Intensifying cooperation between the EU and NATO

International cooperation is essential to counter hybrid threats. Addressing this global phenomenon requires collaboration between the EU and international organisations such as the UN and the OSCE to uphold the rule of law and setting the limits on foreign influence. However, when it comes to practical measures to prevent, detect and respond to hybrid threats, the EU-NATO cooperation is the most relevant, and should be strengthened. In 2017, a common set of proposals for the implementation of the Joint Declaration on EU-NATO cooperation, related to countering hybrid threats, was defined:

- Creation of the European Centre of Excellence for Countering Hybrid threats.
- Enhanced staff-to-staff sharing of time-critical information between the EU Hybrid Fusion Cell and its relevant NATO counterparts.
- Development of technical systems to allow systematic exchange of information.
- Intensified cooperation and undertake shared trend analysis of disinformation.
- Encouragement of cooperation between the NATO Strategic Communication Centre of Excellence and the EEAS StratCom Task Forces.
- Enhanced preparedness for crisis response, seeking to synchronise the two organisations' crisis response activities.
- Raised awareness amongst EU countries and NATO allies on existing and planned resilience requirements, and help them to improve such resilience.
- Implementation of parallel and coordinated exercises (PACE), including hybrid elements.

Since 2017, both institutions have been working hard to implement these proposals. Several progress reports[59] have shown the results of the collaboration between NATO and the EU to counter hybrid threats. However, further efforts are still needed in specific aspects, such as the joint development of automated systems to exchange information and analyse disinformation. Such systems could dramatically improve the capability to prevent and detect hybrid threats.

One of the main instruments to deepen and strengthen such collaboration is the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), which has hosted many meetings, forums, workshops and seminars where both institutions have exchanged their knowledge. However, some EU countries (namely Belgium, Bulgaria, Croatia, Slovakia, Ireland and Malta) do not yet participate in Hybrid CoE activities. These countries are missing out on great opportunities to enhance their ability to counter hybrid threats. The EU should encourage these Member States to participate in Hybrid CoE activities, to ensure similar levels of preparedness to counter hybrid threats as in the EU as a whole.

[59] (NATO - EU Council, 2017a); (NATO - EU Council, 2017b); (NATO - EU Council, 2018); (NATO - EU Council, 2019)

Table 26: Assessment matrix for the policy option 'Intensifying cooperation between the EU and NATO'

Criteria	Adequacy	Argument
Costs and benefits	High	Intensifying the collaboration between NATO and the EU by using advanced technologies to exchange and analyse information would benefit both partners. Although the development of such technologies could be expensive, the benefits would far exceed the costs.
Feasibility	Low	Despite the good relationship between NATO and the EU, the creation of new technical mechanisms to exchange information is limited by political obstacles. Some NATO Allies (mainly the USA) could be reluctant to share information with EU countries that use Chinese technology in their communications infrastructure.
Effectiveness	High	Improving cooperation between NATO and the EU in an issue as crucial as information sharing would undoubtedly contribute to enhancing capabilities in countering hybrid threats. The participation of all Member States in the Hybrid CoE would also increase the EU's resilience as a whole.
Sustainability	Medium	Strengthening collaboration between NATO and the EU by developing technological systems to exchange information would involve significant initial investments. In the medium and long term, those systems should be constantly updated to cope with both the natural progress of digital technologies and the evolving nature of hybrid threats.
Risks and uncertainties	Medium	Past tensions between NATO allies (specifically between the USA and EU countries) regarding public spending on defence could arise again after the Covid-19 crisis, as countries will dedicate further public investment to economic recovery and to improving public health systems, to the detriment of defence spending. The 2020 US presidential election is another relevant milestone for testing NATO allies' willingness to deepen information-sharing.
Coherence with EU objectives	High	This policy is totally coherent with EU objectives, as it seeks to enhance the protection of Member States against hybrid threats. The improvement of international cooperation is highlighted in all EU recommendations and plans as one of the main means to achieve and adequate level of protection.
Potential ethical, social and regulatory impacts	Medium	Strengthening bonds with NATO could provoke social rejection in some EU countries.

6.6.4. Development of training exercises on countering hybrid threats involving all stakeholders

In 2018, the EU Hybrid Exercise Multilayer 18 (EU HEX-ML 18), the first parallel and coordinated exercise (PACE) including hybrid elements, took place. The overall objective was 'to improve and enhance, in a safe-to-fail environment, the EU's ability to respond a complex crisis of a hybrid nature with an internal and an external dimension, as well as to improve cooperation with NATO' (European Council, 2018d, p. 7). The exercise tried to test the EU's ability to deal with international crises that involve components

of hybrid threats such as disinformation, foreign influence, cyberattacks, etc. The exercise involved diverse EU departments from the European External Action Service, the European Commission, the European Council, Member States, and other non-EU participants. However, as hybrid threats affect the whole economy and society, participation in future exercises should not be limited to public bodies but should also include private stakeholders from both fields, particularly those directly involved in dealing with key components of hybrid threats such as disinformation (media outlets, social platforms, etc.) or cybersecurity.

Table 27: Assessment matrix for the policy option 'Development of training exercises on countering hybrid threats involving all stakeholders'

Criteria	Adequacy	Argument
Costs and benefits	Medium	Organising training exercises at the EU level involves relevant costs, while the benefits are difficult to estimate.
Feasibility	Medium	Developing training exercises that involve the private sector is a difficult task. It would entail selecting some representatives who would need to devote significant efforts to preparing themselves for the training exercise, and informing the whole sector about the results.
Effectiveness	Medium	Training exercises can improve the preparedness of public institutions and private stakeholders. However, as the success of hybrid threats is based on their constant evolution (both in terms of content and technical means), the lessons learnt from the training exercises can quickly become obsolete.
Sustainability	Medium	Preparation of training exercises involves great effort for all stakeholders involved, particularly for private companies. Therefore, the periodicity of these exercises would need to be greater than if they only involved public institutions.
Risks and uncertainties	Medium	Private stakeholders could be reluctant to participate in training exercises. Such exercises could be considered an unproductive task with low economic return.
Coherence with EU objectives	High	As hybrid threats try to destabilise the EU and its Member States as a whole, all stakeholders, public and private, should participate in any initiative aimed at countering them. Thus, this policy is aligned with the EU objective of involving the whole economy and society in the fight against hybrid threats.
Potential ethical, social and regulatory impacts	High	This policy does not entail any potential ethical, social or regulatory impact at the EU or national level.

6.6.5. Increasing operational intelligence capability at the EU level

Intelligence services are essential in the fight against hybrid threats. They detect malicious activities in the digital domain that may be related to hybrid attacks, as well as attributing such activity to its real perpetrator. Intelligence services are primarily a national competence and play a key role in the national security strategy of each Member State. The EU Intelligence Analysis and Situation Centre (INTCEN) is the EU body responsible for providing intelligence services in the civilian sphere. The Hybrid Fusion Cell was established in 2016 as part of the EU INTCEN to enhance EU intelligence capabilities and to improve cooperation with Member States' intelligence services.

The EU INTCEN's mandate focuses on providing intelligence-based analysis and assessments (mainly reports and briefings) to EU bodies and policymakers, based on the information collected through open-source intelligence tools (OSINT) and information provided by Member States on a voluntary basis (European Council, 2019a). However, countries are usually only willing to share intelligence information or participate in joint intelligence bodies if they consider that it benefits their interests (Fägersten, B., 2016). Thus, the EU's ability to access intelligence information is limited to what Member States are willing to share, and to the collection through OSINT tools. In this scenario, given that the EU as a whole is increasingly being targeted by promoters of hybrid threats, it would be advisable to increase its operational intelligence capabilities through diverse options:

- Transforming the EU INTCEN into an EU Intelligence Agency with an appropriate budget and resources. The new agency should only be aimed at dealing with EU-related issues, without interfering national intelligence services.
- Leveraging the wide network of EU delegations in third countries to incorporate intelligence staff dependent on the EU INTCEN or the proposed EU Intelligence Agency.

Table 28: Assessment matrix for the policy option 'Increasing operational intelligence capability at the EU level'

Criteria	Adequacy	Argument
Costs and benefits	Medium	Although the costs of improving the EU's operational intelligence capabilities would be very high, it would allow the EU to be better prepared to tackle hybrid threats and support Member States to deal with them.
Feasibility	Low	Intelligence services remain a national competence and Member States could interpret the reinforcement of EU intelligence operational capabilities as interference in their own intelligence services. In fact, some countries have already showed their reluctance towards the creation of an EU Intelligence Agency.[60]
Effectiveness	Medium	The EU's new operational capabilities in the field of intelligence services should be coordinated with national intelligence services. There would be a risk of duplicating structures, which can reduce the effectiveness of the measures adopted.
Sustainability	Low	Increasing operational intelligence capability at EU level could be very expensive in the mid and long term.
Risks and uncertainties	Medium	Bureaucracy could limit the benefits posed by the enhanced operational intelligence capabilities of the EU, as it may slow down responses and reduce their effectiveness.
Coherence with EU objectives	High	As EU institutions and bodies are also being targeted by hybrid threats, the EU itself should have its own operational intelligence capability, in order to address them without having to depend on the willingness of Member States to share information.
Potential ethical, social and regulatory impacts	Medium	Increasing EU operational intelligence capabilities would involve redefining the current role of diverse EU bodies, and new regulation should be enacted to that end.

[60] https://www.politico.eu/article/germany-rejects-creating-european-intelligence-agency/

6.6.6. Development of the European Cybersurveillance Tool (ECT)

An intelligence unit like the Hybrid Fusion Cell, or the intelligence agency proposed in the previous policy option, should encompass involving activities of information collection, processing and analysis as well as reporting for decision making. To achieve their objectives, intelligence units could be supported by a **European Cybersurveillance Tool (ECT**), which is proposed with the aim of establishing the preventive markers, presence indicators and constituent features that will make it possible to identify the new threats looming over cyberspace in an early, consensual and evidence-based manner. The Computer Emergence Response Team for EU institutions (CERT-EU) manages a cyber threat intelligence service (CERT-EU, 2019) and Europol operates the European Cybercrime Centre (EC3).[61] Both services could be the basis for the European Cybersurveillance Tool.

This cybersurveillance tool would facilitate monitoring of open sources, as well as profiling media and social networking entities. To this end, it should have a standardised database for information exchange and data exploitation using mistrust indicators. In this way, the tool would contribute to improving cybersurveillance capacities, allowing what is happening in cyberspace to be monitored and interpreted from a digital perspective.

The modules of this tool may be:

- Collection and analysis of digital sources with harmful content.
- A scorecard, containing all the information necessary for decision-making.
- Risk-based predictive analysis.
- Mechanisms for dissemination of the results obtained to the institutional actors involved (strategic communications).

The European Cybersurveillance Tool should be available to any EU institution or Member State.

Table 29: Assessment matrix for the policy option 'Development of the European Cybersurveillance Tool (ECT)'

Criteria	Adequacy	Argument
Costs and benefits	High	The design, development and operation of the ECT, which is continuously fed with data from the EU and its Member States, would be a significant step forward in countering the threats identified. Although the cost could be high, the benefits would far outweigh it.
Feasibility	Medium	Although the development of the ECT will not entail excessive difficulties, the tool will only be useful if it is permanently fed with data, in near-real time, which may lead to difficulties in implementation.
Effectiveness	High	Real-time analysis of events affecting the EU and its Member States would significantly help the fight against these threats.
Sustainability	Medium	The ECT should be technologically up-to-date, so constant investments would be required.
Risks and uncertainties	Medium	The implementation of a cybersurveillance tool such as the one proposed would require the permanent participation of Member

[61] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

		States, especially in data feeding, which brings a certain degree of uncertainty to the initiative.
Coherence with EU objectives	High	The development and implementation of the ECT is consistent with the EU's objectives, as it would contribute to improving the EU's capabilities in countering hybrid threats.
Potential ethical, social and regulatory impacts	Medium	Enhanced cybersurveillance capacity at the EU level could raise social and ethical concerns regarding respect for fundamental rights such as privacy, freedom of expression, etc.

6.6.7. Increasing public-private collaboration

Private stakeholders are an essential part of the solution to hybrid threats. Most of the information used to prevent, detect, attribute and respond to hybrid threats comes from the private sector. Telecommunication operators, cybersecurity firms, media outlets, social media platforms, utility companies or financial companies, amongst others, have relevant information that would help fight against hybrid threats.

Cooperation between private companies and public authorities in the prosecution of crimes is clearly regulated by national and EU legislation. However, mechanisms for sharing information, gathering evidences or verifying authorship of hybrid threats, which may not be a crime or may not yet have been committed, are less clear. It is, therefore, necessary to create the appropriate regulatory framework and foster dialogue between public authorities and private companies to find the best ways to increase information sharing. In order to encourage the private sector to share the information it collects, public institutions should be able to adequately respond to private companies' legitimate concerns, such as legal liability, and brand reputation due to potential exposure of their own vulnerabilities (Kremidas, C., 2019).

Cooperation between the private sector and public institutions regarding the management of information to counter hybrid threats is not limited to information sharing. Private companies could also collaborate in analysing of such information to detect trends and patterns that could help to prevent hybrid threats. To this end, public and private datasets should be made available to companies, academic and research institutions, civil society organisations and individual researchers. While the re-use of public sector information has mainly been for commercial purposes, it can also be applied to countering hybrid threats. Public institutions should create enough incentives for private agents to collaborate.

Table 30: Assessment matrix for the policy option 'Increasing public-private collaboration'

Criteria	Adequacy	Argument
Costs and benefits	High	Fostering the participation of private agents by both encouraging them to share their information and engaging them in the analysis of public information would undoubtedly contribute to improving the EU's capabilities in tackling hybrid threats. This policy may have a cost for some private companies, but the benefit to the common good far exceeds these costs.
Feasibility	Medium	The EU should create interesting incentives (public recognition, economic support, etc.) to encourage private actors to share their information. However, companies could be reluctant to do so if it affects their business model or puts them at a competitive disadvantage.

Effectiveness	High	Combination of public and private information, as well as increasing the information analysis capability by adding private resources could substantially improve the EU's preparedness to face hybrid threats.
Sustainability	High	Once possible legal barriers are overcome and a cooperation agreement is reached, sustainability over time depends solely on parties' commitment and maintenance of the investment necessary for implementation.
Risks and uncertainties	Medium	Collaboration requires trust. Once the terms of the public-private collaboration have been established, and all parties respect such terms, there should not be any problem. Uncertainties may arise, particularly in certain Member States and/or regions due to a lack of legal certainty and political stability.
Coherence with EU objectives	High	This policy is perfectly aligned with EU objectives, as the fight against hybrid threats involves the whole economy and society. Incentivising the private sector's participation in such a fight is coherent with the holistic approach to tackling hybrid threats that the EU seeks to create.
Potential ethical, social and regulatory impacts	Medium	The private sector's collaboration in identifying authors of hybrid threats may imply the need for legal changes, as well as changes to the terms and conditions of use of some services. Potential conflicts with data protection regulations and limitations to freedom of speech may also arise.

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

6.7.1. Increasing R&D investment and financial support for start-ups, and scaling up companies related to digital technologies

Digital technologies are essential tools in the fight against hybrid threats. However, key applications supporting the creation of strategic communications are developed outside the EU's borders. This increases the risks of misuse of information and data. The recent controversy about the participation of Chinese 5G equipment vendors in the development of European 5G networks is a clear example of the problems that the digital technological gap between the EU and its main competitors can cause. With regards to another technology essential to supporting strategic communications, artificial intelligence, around €3.2 billion was invested in research and innovation in Europe in 2016 by both the public and private sectors. In the same period, around €12.1 billion and €6.5 billion was invested in North America and Asia, respectively (European Commission, 2020c). Clearly, the EU is falling behind when it comes to supporting a critical industry for the security of the Union.

Supporting tech start-ups and helping promising ones to scale up is also indispensable in order to ensure appropriate technological sovereignty and protect the EU against hybrid threats without having to rely on foreign technology. In 2019, European investment in start-ups reached US$34.3 billion, while Asia and the USA reached US$62.5 and US$116.7 billion, respectively (Atomico, 2020). Although the EU has launched diverse funding opportunities for start-ups (like the programme *Startup Europe*), further support is needed if the EU wants to reduce its dependence on foreign technology to protect itself against hybrid threats.

Table 31: Assessment matrix for the policy option 'Increasing R&D investments and financial support for start-ups and scaling up companies related to digital technologies'

Criteria	Adequacy	Argument
Costs and benefits	Medium	The benefits resulting from investment should balance out the economic efforts. A strong European IT industry in key areas to counter hybrid threats and independence from other countries in key infrastructures should be expected. However, initial costs are high while results are expected in the medium and long term.
Feasibility	Medium	These policies have already been developed by the EU. The political commitment of EU Member States should remain unchanged. However, the upcoming economic crisis caused by Covid-19 adds uncertainty to any European budgetary issue.
Effectiveness	Medium	Public funds are expected to produce positive outputs. But economic uncertainty makes it difficult to ensure the effectiveness of policies directly related to the market and industries.
Sustainability	Low	Economic uncertainty makes difficult to guarantee a constant flow of funding in the medium and long term.
Risks and uncertainties	Low	The upcoming economic crisis due to the impact of the Covid-19 puts both the viability of increasing funding and the positive outputs expected from investments at risk. In addition, there are uncertainties surrounding the real and feasible applications of these advanced technologies.
Coherence with EU objectives	High	The options suggested are aligned with the EU's position regarding the relevance of investing in digital technologies for the future of the Union.
Potential ethical, social and regulatory impacts	High	No ethical, social or regulatory impacts have been identified.

6.7.2. Developing industrial policies for key technologies (5G, AI, IoT, blockchain)

The development of industrial policies for key digital technologies is needed to increase the competitiveness of the EU ICT sector and to leverage the impact of economic investments in R&D.

According to a recent ENISA Consultation Paper (ENISA, 2019), there are some aspects of the European ICT industry where the EU can act proactively in order to stablish an ICT industrial policy. As ENISA mentions, the first issue is identifying market segments where the EU ICT industry has the possibility to be competitive. In this case, the segments could include advanced technologies that help counter hybrid threats. The second is keeping the intellectual property developed in Europe within the EU, as well as avoiding the loss of European businesses with high potential by them being taken over by big companies from outside the EU. The third is the use of European standards to turn European diversity (several countries and languages) into a strength. Such issues should be taken into account to develop coherent industrial policies in key technologies for countering hybrid threats, which would undoubtedly contribute to an increase in European technological sovereignty.

Table 32: Assessment matrix for the policy option 'Developing industrial policies for new technologies (5G, AI, IoT, blockchain)'

Criteria	Adequacy	Argument
Costs and benefits	High	Despite the high costs of investments, the benefits obtained from a Tier 1 ICT industry and ICT EU sovereignty would be greater.
Feasibility	Medium	New industrial policy means new negotiations and commitments between Member States. Since certain countries would benefit more than others due to the irregular distribution of the European ICT industry between countries, some Member States could be less willing to commit. In addition, a shift towards national protectionism in order to face the economic consequences of Covid-19 could increase resistance to supporting industrial policies at the EU level.
Effectiveness	Medium	Due to fact that other parties, apart from the EU, participate in ICT competition, the outputs of the policy do only not depend only on the EU performance.
Sustainability	Medium	An ambitious ICT industrial policy involves a huge amount of initial investment, with the expectation of wealth creation in the medium term. With the upcoming economic crisis due to Covid-19, the capacity and willingness of Member States and the EU to carry out such investment could decrease.
Risks and uncertainties	Medium	The main risks and uncertainties come from the performance of EU competitors in the ICT sector (the USA and China) and the current economic and political uncertainty due to Covid-19.
Coherence with EU objectives	High	The Communication from the Commission for a European Industrial Renaissance set out the key priorities for industrial policies. It included innovation and technological advancement as a main source of competitiveness for EU industry (European Commission, 2014a).
Potential ethical, social and regulatory impacts	Medium	Some inequalities between Member States can be displayed and even produced from the development of ICT industrial policies. Developing ICT industrial policies could also lead to the rise of competition issues. New industrial policies could feed protectionist tendencies in Member States, which are already appearing during the management of the Covid-19 crisis.

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

6.8.1. Allowing public authorities to exceptionally intervene in digital services to counteract hybrid threats

Electronic communication laws usually allow public authorities to exceptionally intervene in telecommunication networks and services when specific events affecting public order or national security take place. This authorisation could be extended to also encompass digital services such as messaging services (WhatsApp, Line, Facebook Messenger, etc.), social networks and other widely used applications, with the intention of limiting action taken by promoters of hybrid threats, or warning the population about the effects of such threats.

Table 33: Assessment matrix for the policy option 'Allowing public authorities to exceptionally intervene in digital services to counteract hybrid threats'

Criteria	Adequacy	Argument
Costs and benefits	High	Benefits of the intervention would be high, as it would allow the majority of the population to be informed about an exceptional event related to hybrid threats at a very low cost.
Feasibility	Low	Any private service intervention should be proportionated, carefully assessed and well justified. The intervention can be contested by civil society and providers. Not all EU countries may agree with such interventionist measures.
Effectiveness	High	The effectiveness of the policy would be high, as public authorities could warn large population groups rapidly and at a very low cost.
Sustainability	High	The policy does not involve economic expenditure for public authorities. It could entail costs for digital service providers, but they would not be high.
Risks and uncertainties	Low	This regulation could be risky, as it opens up opportunities for authoritarian governments to use intervention not only when exceptional circumstances occur, but also to suppress any attempt at protest.
Coherence with EU objectives	High	The policy is aligned with the Security Union Strategy 2020-2025.
Potential ethical, social and regulatory impacts	Low	The amendment of telecommunication regulation to extend intervention to digital services could have great regulatory impacts, as well as facing strong social rejection.

6.8.2. Improving law enforcement in 5G networks

According to the report *Internet Organised Crime Threat Assessment (IOCTA) 2018*, produced by Europol, '5G poses a number of particular challenges for law enforcement. The ability of 5G technology to download data from multiples sources (such as Wi-Fi, network towers and satellite) simultaneously will make the investigation of communication events increasingly complex. Moreover, with current 4G technology law enforcement is able to use the unique identifier assigned to a device to attribute the device to an individual, but 5G replaces this with a temporary identifier, making attribution challenging' (Europol, 2018, p. 60). Lawful interception of communications will be more difficult in 5G networks, hindering police work. Promoters of hybrid threats could leverage this issue to act with greater impunity.

The EU should promote the development of tools that help overcome these disadvantages of 5G networks in terms of law enforcement.

Table 34: Assessment matrix for the policy option 'Improving law enforcement in 5G networks'

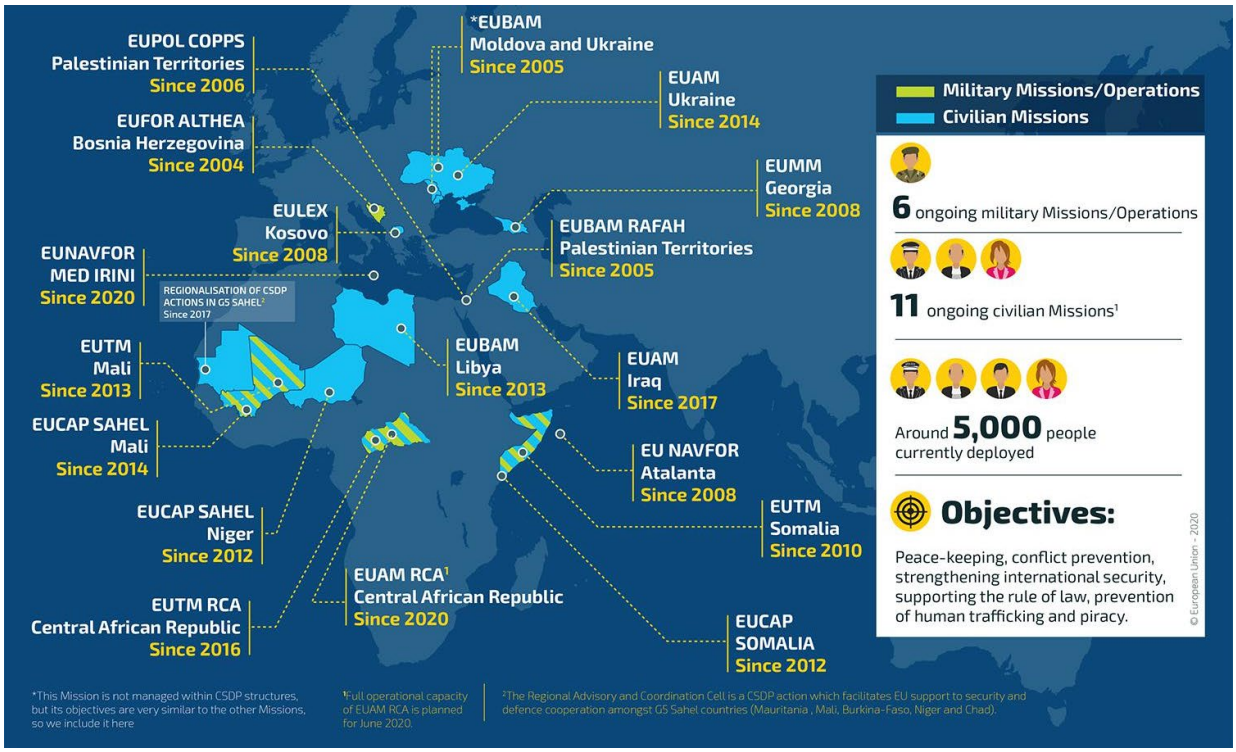
Criteria	Adequacy	Argument
Costs and benefits	Medium	Development costs of technological tools to facilitate lawful intervention in communications could be very high. However, the benefits of improving law enforcement would also be high for society security.
Feasibility	Medium	5G networks are already operative in many countries and standards are not easy to modify. Additional technical solutions will have to be developed to support police work.
Effectiveness	High	Improving law enforcement in 5G networks will contribute to detecting and preventing attempts to use such networks for developing hybrid attacks.
Sustainability	Low	Technical solutions may require constant updates to cope with criminals' ability to leverage the potential of 5G networks. This could involve high costs.
Risks and uncertainties	Medium	Criminals are increasingly sophisticated and could be capable of leveraging 5G networks get ahead while the police try to catch up technologically.
Coherence with EU objectives	High	The policy is aligned with the Security Union Strategy 2020-2025.
Potential ethical, social and regulatory impacts	High	No ethical, social or regulatory impacts are identified, as this is a technical upgrade to systems and applications that already work in 4G networks.

6.9. Policies aimed at defining proactive approaches to dealing with hybrid threats

6.9.1. Strengthening the EU's vision and values outside the EU borders

The EU carries out an intense external action through CFSP (Common Foreign and Security Policy) and CSDP (Common Security and Defence Policy) instruments to help foreign countries deal with humanitarian crises, stand for human rights, reinforce democratic institutions and peace processes in conflictive areas, and to strengthen close cooperation and engagement with neighbouring countries. The following figure summarises the CSDP's ongoing missions and operations:

Figure 10: EU CSDP missions and operations 2020



Source: European External Action Service

Regarding the global strategy of the EU's Foreign and Security Policy, mechanisms such as those included in the FPI's (Foreign Policy Instruments) financial toolbox and the FPI's regulatory toolbox[62] are used to promote democracy, build alliances, prevent conflicts and respond to crises.

All these instruments should be used to spread the EU's vision and values across the world. Specific communication strategies should be included, with adequate budget and staff, to promote the EU's principles and worldview amongst diverse audiences (citizens, policy-makers, politicians, civil society organisations) in the countries where such instruments are deployed. The Strategic Communications division at the EEAS, as well as its task forces, should actively collaborate in the definition and implementation of such strategies.

Table 35: Assessment matrix for the policy option 'Strengthening the EU's vision and values outside EU borders'

Criteria	Adequacy	Argument
Costs and benefits	Medium	The cost of implementing effective strategic communications in CFSP missions can be high. Additionally, the benefits of such strategy are usually expected in the mid and long term.
Feasibility	High	As strategic communications are gaining momentum to counter hybrid threats, it is a good time to incorporate them into the EU's external action missions.
Effectiveness	Medium	Changing minds and beliefs is a complex and long-term task. Communication strategies should not be limited to occasional and isolated activities to be effective.

[62] https://ec.europa.eu/fpi/what-we-do_en

Sustainability	Low	Proactive strategic communications should be maintained over a long time to be effective. This would imply sustained economic effort after the mission is accomplished.
Risks and uncertainties	Medium	Policy-makers usually seek results in the short term, so they may rule out measures whose goals can only be achieved in the mid and long term.
Coherence with EU objectives	High	The spreading of the EU's values and worldview is totally coherent with EU objectives, which seek to extend democracy and the rule of law all over the world.
Potential ethical, social and regulatory impacts	Medium	The EU could be accused of wanting to extend its worldview without respecting local characteristics and traditions.

6.9.2. Supporting free journalism against disinformation

Free journalism and media freedom are key pillars of democracy and essential instruments to counter hybrid threats, particularly disinformation. Free journalism contributes to developing better informed and more engaged citizens, who are more aware of the existence of disinformation and, therefore, less likely to be influenced by it. Free journalism is also necessary to guarantee freedom of expression and the ideological plurality that characterises democracies. In this sense, supporting free journalism can be deemed a proactive measure to improve society's resilience to disinformation and any attempt to restrict freedom of expression.

The EU has already defined diverse tools to promote and support free journalism:

- In 2014, the Council enacted the EU human rights guidelines on online and offline freedom of expression (European Council, 2014). The guidelines included diverse instruments (monitorisation, financial aids, diplomatic support, etc.) to improve free journalism in EU and candidate countries.
- The European Commission has implemented several actions to promote media freedom and pluralism: support for the Centre for Media Pluralism and Media Freedom[63] to monitoring risks for free journalism; definition of guidelines for EU support for media freedom and media integrity in enlargement countries; economic support for media freedom projects.[64]
- The European External Action Service annually supports World Press Freedom Day.

Despite these efforts, free journalism and media freedom are still threatened in many countries. Although there are significant levels of free journalism within the EU (with some exceptions),[65] press freedom in the main promoters of disinformation is almost inexistent. While Russia ranks 149th out of 180 countries, in the 2020 World Press Freedom Index of the NGO Reporters Without Borders, China ranks 177th. In the countries where most disinformation is created, there is hardly any counterbalance in the form of free journalism.

Acknowledging the great work done by the EU to promote free journalism across the world, further efforts are still needed in the countries most vulnerable to disinformation. Although the EU may have

[63] https://cmpf.eui.eu/media-pluralism-monitor/

[64] https://ec.europa.eu/digital-single-market/en/media-freedom-projects

[65] According to the 2020 World Press Freedom Index, produced by the NGO Reporters Without Borders, 15 of the top-30 countries are EU countries. However, 5 EU countries (Poland, Greece, Malta, Hungary, Bulgaria) are outside the top-60. For more information visit: https://rsf.org/en/ranking_table?sort=asc&order=Ranking

little opportunity to support free journalism in countries that lead in terms of disinformation (Russia and China), it should focus its efforts on those countries under the influence of disinformation leaders, mainly former Soviet Republics and African countries.

Table 36: Assessment matrix for the policy option 'Supporting free journalism against disinformation'

Criteria	Adequacy	Argument
Costs and benefits	High	Improving media freedom and free journalism in the countries most vulnerable to disinformation can contribute to limiting its effects. The cost would not be too high.
Feasibility	High	This policy option should not raise any concern at the political level. Its practical implementation could be more difficult and adequate instruments (funds, collaboration with EU journalists and media outlets, etc.) should be defined.
Effectiveness	Medium	Free journalism can improve citizens' levels of awareness about disinformation and thus hamper its goals. However, the results are not immediate and could take a long time to materialise.
Sustainability	High	As costs to support media freedom would not be very high, actions could be maintained over time.
Risks and uncertainties	Medium	Some current policy trends (rising populist movements, polarisation of society, shifts in the geopolitical arena after the Covid-19 crisis) can lead to reduced citizens' confidence in media outlets and press. Thus, measures to promote media freedom could be useless.
Coherence with EU objectives	High	Freedom of expression and information is enshrined as a fundamental right in the EU, so any measure aimed at promoting such freedom, both inside and outside EU borders, is totally coherent with EU objectives.
Potential ethical, social and regulatory impacts	High	This policy option would not involve any ethical, social or regulatory concern.

6.9.3. Mandatory creation of StratCom units at the highest level in EU countries and institutions

Any EU country or institution that seeks to adapt its response to hybrid threats in the informational arena from a reactive to a proactive approach should have a coherent and clear communication strategy. Strategic communications are key elements in countering disinformation, and all EU countries and the main EU institutions should create units devoted to defining, implementing and monitoring them at the highest level. Such units should control the flow of information from the country or institution to the public. They should also be responsible for coordinating all activities related to collecting intelligence and knowledge about potential threats, defining the appropriate strategy and timing to spread the information, and engaging diverse stakeholders (media outlets, civil society, influencers, enterprises, etc.) to improve the impact of communications. These units should be made up of communication professionals, intelligence experts, military experts, technicians specialised in data analytics and artificial intelligence, representatives from the civil society and the economic sector, amongst others. The units should have enough competencies to access information, to some extent, from different departments (domestic and foreign affairs, defence, economy, and others) and to lead

them when specific campaigns are developed. The EU should urge Member States and its own institutions and agencies to create such units. In order to improve their efficiency and coordination, specific guidelines about the objectives, competences, structure, and operation should be prepared by the EU.

Table 37: Assessment matrix for the policy option 'Mandatory creation of StratCom units at the highest level in EU countries and institutions'

Criteria	Adequacy	Argument
Costs and benefits	Medium	The costs of creating StratCom units at the highest level in all EU countries and institutions would be high while the benefits would depend on how such units are managed.
Feasibility	Low	Member States could consider strategic communications as a national competence, and the EU could not oblige them to create such units. Additionally, other institutions inside national governments may not be willing to share information with those units, hampering its operations.
Effectiveness	High	StratCom units could help Member States and EU institutions to improve their communication capacities, unifying actions in a single body and making them more effective.
Sustainability	Low	The costs of maintaining StratCom units would increase over time, as they would have to be technologically up-to-date to properly deal with evolving hybrid threats.
Risks and uncertainties	Low	StratCom units should be left out of the political struggle and should maintain stability beyond each term, avoiding their politicisation.
Coherence with EU objectives	High	StratCom units in Member States and EU institutions would facilitate the fight against disinformation, improving coordination and unified responses in the whole EU.
Potential ethical, social and regulatory impacts	Low	The creation of StratCom units would have relevant regulatory impact, as diverse national legislation should be modified to facilitate information-sharing between departments.

6.9.4. Creation of an EU news agency to ensure veracity of information

After 2019, when measures to combat disinformation linked to the numerous electoral processes throughout the EU seemed to have been successful, the Covid-19 crisis has led to the outbreak of harmful disinformation campaigns that have affected diverse Member States and the EU as a whole. Recent examples, such as the false accusation that 5G networks spread the coronavirus, which has led to arson attacks against mobile phone masts in several EU countries (Cerulus, L., 2020), or the false recommendation to drink bleach to protect oneself against the coronavirus, show their growing danger. As the High Representative of the Union for Foreign Affairs and Security Policy declared, 'disinformation can kill' (disinfo.eu, 2020).

EU attempts to debunk disinformation have been so far limited and with scarce impact on public opinion. The most important initiative (the website EUvsDISINFO, created by the EEAS East StratCom Task Force) is only focused on debunking Kremlin disinformation operations against the EU, and it only offers all the information in English and Russian (a small amount of content related to the Covid-19 has been translated into German, French, Italian and Spanish). Given the growing impact of disinformation related to Covid-19 amongst European citizens, the European Parliament itself, in a resolution on the

EU coordinated action to combat the Covid-19 pandemic and its consequences, urged the EU 'to establish a European information source, in all official languages to ensure that all citizens have access to accurate and verified information' (European Parliament, 2020, p. 11). This kind of European information source, which could take the form of an EU news agency, should be the official voice of the EU and all EU institutions should follow its guidelines when communicating, not only during the Covid-19 crisis but also when dealing with future disinformation campaigns.

Table 38: Assessment matrix for the policy option 'Creation of an EU news agency to ensure veracity of information'

Criteria	Adequacy	Argument
Costs and benefits	Medium	The costs of creating a unique source of information for the whole EU in all EU official languages would be very high. However, it would allow to offer an image of unity of all EU institutions which could reinforce the messages transmitted.
Feasibility	Low	It would be very difficult for all EU institutions to leave their communication in the hands of an independent body. Coordination between the new EU news agency and other institutions would be highly complex.
Effectiveness	High	Journalists, media outlets, policy-makers and any other stakeholder could have a unified source of information related to EU matters, and verifying of the information would be much easier.
Sustainability	Low	The creation of this kind of EU body would involve high costs in a context of budget reduction and economic crisis due to the Covid-19 pandemic.
Risks and uncertainties	Low	The creation of this kind of EU body would involve high costs and some political parties may prefer to allocate their budget to other areas.
Coherence with EU objectives	High	The EU news agency would be highly aligned with EU objectives of combating disinformation and reinforcing the EU's image abroad.
Potential ethical, social and regulatory impacts	Medium	The EU news agency could collide with national public agencies and other institutions devoted to ensuring the veracity of information (fact-checking initiatives). The creation of such an agency would also require intense regulatory work to oblige other EU institutions to collaborate.

6.9.5. Improving diplomatic relations with countries considered strategic challenges

The European Union's values in the field of security and diplomacy include promoting stability, security, prosperity, democracy, fundamental freedoms and the rule of law at the international level. That is why the EU cannot remove any country from its diplomatic work, even if its activity could be considered a strategic challenge. Additionally, the economic ties between the EU and some of the countries most actively promoting hybrid threats (China and Russia) are so tight that the best way to reduce such threats could be to improve diplomatic relations.

Relation with Russia, which was a 'strategic partner' of the EU between 1991 and 2014, has become 'the most important strategic challenge for the EU' (European External Action Service, 2016a). At the international level, both the United States and France have made diplomatic approaches to Russia, in

an attempt to re-integrate it again as a member of the G8, from which it was expelled after the annexation of Crimea (Atwood, K. & Klein, B., 2019).

Over the last few years, China and the EU have also moved closer together on major issues on the global agenda such as the defence of free trade, global sustainable development and multilateralism (European Commission and the High Representative, 2019). At the press conference on the EU-China Strategic Dialogue in June 2020, the High Representative, Josep Borrell, highlighted the need to have a balanced and reciprocal approach to this cooperation, in areas such as connectivity, free trade, scientific cooperation, and also media and cultural cooperation. He stressed the need to 'engage with China to achieve our global objectives, based on our interests and values' (European External Action Service, 2020).

Further development of diplomatic relationships with both countries could be a way to reduce the state-sponsored hybrid threats coming from them.

Table 39: Assessment matrix for the policy option 'Improving diplomatic relations with countries considered strategic challenges'

Criteria	Adequacy	Argument
Costs and benefits	High	Establishing protocols and diplomatic measures in order to be able to solve possible disputes without resorting to hybrid threats could benefit the EU without incurring excessive costs.
Feasibility	Low	Although the EU and some of its Member States are gradually trying to draw closer to certain countries that are considered a strategic challenge, it is important that the EU does not give in on its principles, values and organisational cohesion. The EU's vision and values are so different from those of challenging countries that diplomacy alone would not be enough to prevent hybrid threats from those countries.
Effectiveness	High	If certain diplomatic approaches could be reached between the EU and Russia and China, the hybrid attacks from those countries against the EU and its Member States could decrease.
Sustainability	Low	While ideally all disputes would be resolved through diplomatic channels, not all problems can be solved equally. New controversies between the EU and Russia and China, which might not be solved by diplomatic means, could periodically trigger new hybrid threats.
Risks and uncertainties	Low	The risks are also high as diplomatic solutions can lead to the EU being perceived as weak in the international sphere.
Coherence with EU objectives	Medium	As we have already pointed out, the EU cannot surrender its principles to countries whose democracy is questioned (or is not democratic at all) and whose values may not coincide with those of the Union. That is why establishing a dialogue with actors who may attack the basic pillars of the rule of law or democratic principles cannot always be possible.
Potential ethical, social and regulatory impacts	Medium	Dialogue and diplomacy are essential and unquestionable values within the EU and should always be the first option considered when resolving any kind of international conflict. However, entering into dialogue with countries that have little respect for human rights might be perceived as inconsistent by European society.

7. Conclusions

Hybrid threats: a growing menace to the EU

The hybrid threats that European countries have faced, and still face, have specific objectives that seek to harm them as individual targets, but they are also part of an overall strategy to destabilise the EU (Fiott, D. & Parkes, R., 2019). As a result, the EU has launched numerous initiatives[66] at the strategic, tactical and operational levels, especially since 2014, aimed at responding to the hybrid threats faced by its Member States and its neighbouring countries.

From the point of view of information and communications, the main pillar of EU action to counter hybrid threats is the fight against disinformation. As we have already seen, disinformation is defined by the European Commission as 'verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm' (European Commission, 2018b, p. 3). It seeks to undermine citizens' trust in democratic processes and institutions, including electoral systems, intensifying political polarisation, challenging social cohesion or social models and generating confusion about geopolitical events. Its ultimate goal is to destabilise the target: both the country or region attacked and the EU as a whole.

Strategic communications: an appropriate means to deal with disinformation

Strategic communications comprise a 'systematic series of sustained and coherent activities, 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' (Tatham, S., 2008, p. 3). They are considered one of the main ways to respond quickly and effectively to disinformation campaigns. Therefore, they have become one of the top priorities of European security policy and external action.

In brief, the actions implemented by the EU so far aim at:

- Enhancing cooperation and information-sharing between Member States and EU institutions to identify and jointly respond to disinformation.
- Mobilising the private sector to tackle disinformation (technology providers, digital platforms, social networks, advertisers and the advertising industry).
- Supporting high quality information by empowering journalists and fact-checkers to deal with disinformation.
- Raising awareness and media literacy amongst citizens.

Nevertheless, analysis of the evolution and chronology of Europe's response to the growing impact of hybrid threats shows that it has been largely reactive, and the EU still lacks an offensive, and not merely defensive, strategic communication response to these threats (European Parliament, 2016d).

As Daniel Fiott and Roderick Parkes pointed out in a recent Chaillot Paper from the European Union Institute for Security Studies (EUISS), some relevant aspects of European action against hybrid threats remain to be addressed:

- The exchange of information and intelligence between Member States and between the institutions of the European Union is still an incipient work.

[66] See chapter 3.4.1

- The need to overcome EU institutions' fragmentation and silo mentalities when developing their strategies.
- Risk assessments are often based on a minimum level of information exchange.
- Appropriate and coordinated responses are still hindered by a significant lack of trust (Fiott, D. & Parkes, R., 2019).

An overall strategy to tackle hybrid threats is needed

A European response must include joint political and diplomatic, informative and intelligence, economic, legal and military actions. These actions have to focus on the case investigation and clarification of responsibilities, as well as the deployment of sanctions, as well as on identifying future risks and increasing the European economic and technological independence from risk countries or providers. Adequate investment in technological developments to anticipate new threats is at the core of a preventive policy.

Currently, the main source of disinformation in Europe is Russia (European Parliament, 2019). However, shifts in the international balance of power raise concerns about China's growing soft power and capacity for influence capacity. Unlike Russia, China is playing a critical role in the global digital sector, particularly in the deployment of 5G networks in Europe. As both hybrid threats and strategic communications to counter them rely more and more on digital means, China is increasingly becoming a major actor when dealing with such topics.

The double role played by digital technologies regarding hybrid threats

As previously described, digital technologies open up great opportunities to spread messages amongst broad audiences in a rapid and inexpensive way, and to create customised narratives for very specific audiences. Digital technologies can be used by both the promoters of hybrid threats, to fabricate and spread disinformation, and by the institutions that fight them to develop counter-narratives. The following table summarises the diverse characteristics, as highlighted in previous sections, of the most relevant technologies and applications (5G networks, social media, artificial intelligence and blockchain), and the benefits they bring to both promoters and defenders.

Table 40: Potential usefulness of digital technologies in the realm of hybrid threats

5G		
Characteristic	**Benefits for attackers**	**Benefits for defenders**
Increase in connection speed	Possibility to increase the dissemination of harmful/malicious content or disinformation in high quality video format.	Possibility of responding to attacks with mass fact-checking campaigns, or the rapid dissemination of truthful messages in high-bandwidth consumption formats (for instance, high quality videos).
	Increased communication capabilities amongst malicious actors, for the purposes of preparation, dissemination and attack.	Increase in strategic communication capacities amongst different EU actors, for the purposes of prevention, detection and response.
Reduction of latency time	Possibility to increase the dissemination of harmful/malicious content or disinformation with fewer delays.	Possibility of increasing the response to attacks with fewer delays.

Reduction of energy consumption	Possibility of increasing attacks, at a lower cost, or helping attackers keep a low exposure profile.	Possibility of increasing response mechanisms (strategic response communications) to attacks, at a lower cost.
Increase in the number of devices supported by a network	Increased ability to develop multiple attacks, using a multiplicity of devices.	Possibility for a multiplicity of devices to cooperate in mitigating the effects of attacks.
Integration with the Internet of Things	Possibility that the attacks also target smart devices, or that such devices may be part of a larger scale attack.	Increase in elements aimed at counteracting the effects of attacks.
Social Media		
Characteristic	**Benefits for attackers**	**Benefits for defenders**
Universality and mass usage	Possibility of greatly increasing the dissemination of harmful/malicious content or disinformation.	Possibility of responding to attacks with massive fact-checking campaigns or dissemination of truthful messages.
	Increased communication capabilities amongst malicious actors, for the purposes of preparation, dissemination and attack.	Increase in strategic communication capabilities between different EU actors, for the purposes of prevention, detection and response to attacks.
	Possibility of using social networks as a mechanism for the dissemination of malicious code (malware) and the perpetration of other types of attacks (e.g. ransomware).	
Access from multiple devices (PCs, tablets, smartphones)	Development of attacks with multiple origin, using a multiplicity of devices.	Possibility for a multiplicity of devices to cooperate in mitigating the effects of attacks.
Artificial Intelligence		
Characteristic	**Benefits for attackers**	**Benefits for defenders**
Adaptive technology	Possibility of designing tailor-made attacks (evading detection, hiding where they cannot be found and automatically adapting to countermeasures), taking into account the specific characteristics of the victims and their environment.	Possibility of designing tailor-made defence mechanisms, taking into account previous knowledge of the attackers, behaviour patterns, etc.
Ease of access to AI systems and applications	Possibility of increasing the dissemination of harmful/malicious content or disinformation, with greater guarantees of success.	Possibility of responding to disinformation campaigns or cyberattacks, with greater guarantees of success
Natural language processing and machine translation	Increase in the capacity for relationships and communication between international attacking groups.	Increase in the relationship and communication capacities between the different EU actors responsible for preventing, detecting or mitigating the effects of attacks.

Deepfakes and GAN networks	Increased impact of attacks and disinformation, with the use of audio, photo or video deepfakes, and the use of GAN networks to crack passwords, evade malware detection or trick facial recognition.	GAN networks can also be used for the opposite purpose: to avoid password cracking, malware detection or deepfake detection.
Cybervigilance Technology Observatories		Possibility to increase analysis of disinformation campaigns in real time and in an early manner, responding immediately and facilitating decision-making.
Blockchain		
Characteristic	**Benefits for attackers**	**Benefits for defenders**
Monitoring of transactions and content		Possibility of designing mechanisms to track the origin and destination of the contents of disinformation campaigns.
Less dependence on media	Possibility of developing attacks without the need to link the content to any media.	Possibility of decentralised verification of the contents of disinformation campaigns.

Source: Own elaboration

According to different sources,[67] Europe is falling behind (or at risk of falling behind) its main competitors (the USA and China) regarding the development of such technologies, leaving the control of essential digital tools used to counter hybrid threats and, particularly disinformation, in foreign hands. Thus, further EU efforts to achieve technological sovereignty in these crucial technologies (von der Leyen, U., 2019), boosting research and development as well as the creation of European digital leader companies, are also critical to address these threats.

Some challenges remain unresolved

In summary, the main challenges faced by the European Union in facing regarding the communication aspects of hybrid threats are:

- Better and faster coordination amongst EU institutions and national authorities: sharing high quality intelligence and information and common actions against promoters of hybrid threats.
- Adopting more proactive approaches instead of reactive measures.
- Counterbalancing effective measures with key European democratic values such as freedom of expression and transparency, in a context of a lack of clear leadership.
- Reinforcing the role of private actors in the fight against disinformation:
    - Social media
    - Traditional media, journalists, fact checkers and civil society
    - The digital industry
- Improving EU technology sovereignty and reducing technological dependence on other countries, mainly the USA and China.

[67] (Bughin, J. et al., 2019); (Northstream, 2019); (Ekholm, B., 2019);

- Strengthening the role of citizens: raising awareness, literacy.

Actual implementations of hybrid threats usually rely on a limited set of actions

Some interesting questions arise from analysis of the case studies, with the following being the most relevant: at what point can an attempt to meddle in the victims' interests be classified as a hybrid threat? Where is the line between a legitimate foreign influence and a hybrid threat? While the most accepted definitions of hybrid threats[68] give some clues about the characteristics that any action should fulfil to be considered as such, it is also true that there are very few examples of hybrid threats that meet most of these features. Probably the only example of a hybrid threat that encompasses all the characteristics is the illegal Russian attack against Ukraine to conquer Crimea. This case, the most paradigmatic one, implemented a wide array of coordinated and synchronised actions (cyberattacks, covert armed groups, disinformation campaigns, economic pressure, psychological operations against Ukrainian soldiers, religious matters, etc.). It had a clear strategic goal (to achieve the annexation of Crimea at minimum cost in military terms), and exploited the target's vulnerabilities (political instability after the Euromaidan demonstrations), and influenced the political decision-making process (reversing the rapprochement to the EU in Ukrainian regions under Russian influence). No other case has deployed so many components of hybrid threats. However, all the cases considered help us draw useful conclusions about the use of strategic communications to counter hybrid threats.

The blurred line between influence and interference

The cases analysed reflect the difficulty of differentiating between foreign influence and foreign interference when hybrid tools are used. While all governments in the world seek to influence others, which is not necessarily bad practice, foreign interference also includes coercive, corrupting, deceptive and clandestine activity, and it is contrary to the victim's sovereignty, values and national interests. The cases show how actions that could be considered as legitimate foreign influence (spreading a religious belief, seeking military support) end up becoming foreign interference by adopting the form of a hybrid threat.

Two complimentary objectives of hybrid threats

Hybrid threats are always deployed to achieve a strategic goal while undermining the target, aiming to interfere in decision-making or democratic processes. However, as the cases analysed (except for the case of Ukraine) are what we could call 'partial' examples of hybrid threats,[69] some of them are more oriented towards strengthening one's own position while others are aimed at destabilising the victim. We can, therefore, distinguish between two types of cases. On the one hand, we find cases where the threat is focused on undermining the target and the final strategic objective is not so direct or immediate (the case of Lithuania, the Netherlands or Spain). In these cases, the perpetrator tries not to be detected and attribution is complex, as the lack of attribution is in itself a key component in these attacks. Knowing that a disinformation campaign on a regional issue was of foreign origin would, for example, detract from its credibility and impact, and its intention to interfere in internal affairs would be evident.

On the other hand, threats oriented towards reinforcing the strategic position or amplifying the influence of the attacker on a country or region (like Chinese and Russian soft power in Western democracies through academic institutions and think tanks, Saudi pressure on Pakistan or the Zapad military exercises) can also be found. In these cases, the perpetrator is known, but the intentions and strategies exploit the thresholds between legitimate influence and interference.

[68] See Chapter 2.1

[69] We have used the term 'partial' as each hybrid threat analysed only encompasses a limited number of components compared to the most paradigmatic case, the Russian aggression against Ukraine.

Different attack vectors aimed at diverse objectives and targets

Analysis of the cases shows an interesting relationship between the means (or attack vectors) deployed over the course of a hybrid threat, and the nature of the targets. When the purpose of the hybrid threat is to destabilise the victim by generating confusion, mistrust or social disapproval of its government or institutions, it is aimed at broad targets (for instance the Muslim community in the Netherlands, the Ukrainian population in Crimea and neighbouring areas, the Lithuanian and Catalonian populations). In these cases, promoters use massive online media outlets and social networks to spread their narratives. These means of action facilitate concealment of the authorship of the attack.

However, when it comes to strengthening one's position and increasing one's influence, specific targets are preferred (Pakistani authorities, academic institutions and academic and political elites in the case of the Confucius Institute and Russian think tanks and NGOs), and the attackers rely more on face-to-face communication (meetings, conferences, seminars, diplomatic channels, etc.) and financial pressure.

In the realm of communication, disinformation campaigns are the most frequent component

At least four out of the seven case studies involve any kind of disinformation campaign. Promoters of hybrid threats take advantage of the great opportunities opened up by social networks to spread false content aimed at supporting their claims and goals. All disinformation campaigns share similar characteristics: they are built around false news related to nefarious crimes ('crucifixion of a boy by Ukrainian soldiers', 'rape of a teenage girl by German soldiers') or exacerbated confrontations ('tanks on the streets of Barcelona'); they appeal to people's feelings and sentiments, inciting hatred of the other (Dutch society, Ukrainians, the German soldiers, the Spanish government, etc.); they use false accounts and bot networks to amplify the impact of the false information. Of all the disinformation campaigns analysed, one stands out for its use of innovative elements to amplify its impact: the one promoted by the Catalan pro-independence movement. They used public figures with allegedly great credibility and reputation on social networks (Julian Assange) or with many followers (Pamela Anderson) to support their claims and achieve high impact.

One of the case studies only involved disinformation campaigns: the attempts to discredit the NATO mission (Enhanced Forward Presence) in Lithuania by making false accusations of German soldiers raping a teenage girl. The question that arises here is: can a disinformation campaign constitute a hybrid threat on its own? In our opinion the response should be affirmative, and that is how the authorities who had to deal with it understood it. If a disinformation campaign seeks to undermine citizens' trust in democratic institutions and related organisations, like NATO, and tries to meddle in democratic processes and decisions (such as Lithuania's request for NATO's help), it fulfils two of the essential characteristics of hybrid threats and should be considered as such.

Proactivity and cooperation, key elements of strategic communications to counter hybrid threats

Few examples of the communication strategies developed to counteract the attacks in the case studies can be considered successful. In the case of the illegal annexation of Crimea by Russia, Ukraine could hardly respond to such a demonstration of hybrid force. Moreover, the fact that Ukraine did not have a clear communication strategy with specific objectives and preventive informative actions for the diverse stakeholders involved (Ukrainian citizens, soldiers, international community) also contributed to the success of the Russian narrative presenting Ukraine as a failed country unable to help its citizens, which, in turn, was used as an excuse to annex Crimea. In Catalonia, the Spanish authorities did not have a communication strategy to counteract secessionist disinformation until well after the illegal independence referendum. Only in the face of the deterioration of Spain's public image in the international arena following the events of the illegal referendum, was a tepid reactive communication strategy defined. Both examples show the difficulty of creating an effective communication strategy when the promoters of hybrid threats have long-term objectives. However, adopting a merely reactive

attitude, leaving the initiative to the promoters of hybrid threats and focusing on debunking disinformation, helps the attacks to achieve their objectives.

In two cases, the Pakistan's refusal to participate in the Yemeni Civil War and the disinformation campaigns against NATO in Lithuania, the victims adopted successful strategic communications to counter threat promoters' objectives. In both cases, these objectives were specific and short-term. In the case of the disinformation campaigns against NATO in Lithuania, the previous work (preventive measures) conducted by the Baltic country to raise awareness amongst its citizens, politicians and civil servants about potential Russian meddling in its home affairs was very effective in swiftly reacting to and limiting the effects of false information. Close cooperation amongst the main stakeholders (Lithuanian authorities, German Army and NATO) was another key to success.

In the case of Pakistan, the main driver behind its communication strategy was the coherence of the message. Pakistan insisted on its intent to remain neutral in the Yemeni conflict, despite the intense pressure it was subjected to. Even when it conceded to the Saudi requirements and finally sent troops to the Arab country, it remarked that they were not going to participate in the war.

Another case with a relatively successful communication strategy is the Dutch strategy to counter Salafi propaganda. Although it is not yet possible to verify its effectiveness, it does include most of the elements of strategic communications, as it has long-term aims (beginning to debunk Salafi propaganda from childhood), intends to address diverse groups (young people, families, imams, mosque administrators, teachers, etc.) with specific messages for each of them, built on tailored narratives and provided through a full spectrum of means (offline and online).

Analysis of these cases has revealed strategic communications' potential to counter hybrid threats. However, few victims (whether they are countries, academic institutions, specific groups, etc.) have been able to take advantage of this potential so far. More proactive approaches, better cooperation and more intensive use of digital technologies are needed to provide more efficient and effective responses to hybrid threats.

Comparative analysis of the policy options

After individual analysis of the proposed policy options, conducted in Chapter 6, a comparative assessment of these policy options may help policy-makers to identify which are most suitable for development. The following table shows the ranking of the policy options according to their adequacy in accordance with the assessment criteria. Each criterion has been given a weight based on its relevance, which has been used to calculate the overall score for each policy. The score also depends on how adequate (high: green arrow; medium: orange dash; low: red arrow) the policy is for the specific criteria.

Table 41: Summary of the policy option assessment

Type	Policy	Criteria: Costs and benefits	Feasibility	Effectiveness	Sustainability	Risks and uncertainties	Coherence with EU objectives	P. ethical, social and regul.	Overall assessment (1 to 100)
		Criteria weigth (1 to 10)							
		8	10	10	6	4	6	4	
Awareness raising	Policymaker training	↑	↑	↑	↑	↑	↑	↑	100
Regulation	Regulation of risk analysis for hybrid threats	↑	↑	↑	↑	↑	↑	–	96
Awareness raising	Promoting citizen guides to detecting disinformation	↑	↑	↑	–	↑	↑	↑	94
Regulation	Improving regulation of artificial intelligence to address hybrid threats, disinformation and foreign interference	↑	↑	↑	↑	–	↑	–	92
Regulation	Development of the European Strategy against Hybrid Threats, Disinformation and Foreign Interference (EU-HTDFI Strategy)	↑	–	↑	↑	↑	↑	–	85
Proactive approach	Supporting free journalism against disinformation	↑	↑	–	↑	–	↑	↑	85
Awareness raising	Teacher training and ongoing development of educational resources and content	↑	–	↑	↑	↑	–	↑	83
Social media platforms	Making the Code of Practice on Disinformation mandatory, and adding periodic external audits	–	↑	↑	↑	–	↑	–	83
Awareness raising	Incorporation of critical information analysis competencies in school curriculums	↑	–	↑	↑	–	↑	–	81
Coordination	Creation of a coordination unit at the EU level to unify responses against hybrid threats	↑	–	↑	↑	–	↑	–	81
Coordination	Increasing public-private collaboration	↑	–	↑	↑	–	↑	–	81
Coordination	Development of the European Cybersurveillance Tool (ECT)	↑	–	↑	–	–	↑	–	75
Coordination	Creation of common response mechanisms at the EU level	↑	↓	↑	↑	–	↑	–	71
Regulation	Update the interpretation made by the Cybercrime Convention Committee (T-CY) regarding interference in electoral processes	↑	↓	↑	↑	↑	↑	↓	71
Regulation	Adaptation of a sanction regime against promoters of hybrid threats, disinformation and foreign interference	↑	–	↑	–	–	–	–	69
Awareness raising	Digital literacy programmes for people with low digital competency	–	–	–	–	↑	↑	↑	65
Technology gap	Developing industrial policies for key technologies (5G, AI, IoT, blockchain)	↑	–	–	–	–	↑	–	65
Coordination	Intensifying cooperation between the EU and NATO	↑	↓	↑	–	–	↑	–	65
Use of digital channels	Improving law enforcement in 5G networks	–	–	↑	↓	–	↑	↑	65
Use of digital channels	Allowing public authorities to exceptionally intervene in digital services to counteract hybrid threats	↑	↓	↑	↑	↓	↑	↓	63
Coordination	Development of training exercises on countering hybrid threats involving all stakeholders	–	–	–	–	–	↑	↑	60
Attribution	Increasing economic resources allocated to the attribution of threats	–	↓	↑	–	↑	↑	–	60
Proactive approach	Strengthening the EU's vision and values outside the EU borders	–	↑	–	↓	–	↑	–	60
Regulation	Improvement and harmonisation of the European legal framework against hybrid threats, disinformation and foreign interference	↑	↓	↑	–	↓	↑	↓	56
Attribution	Increasing economic resources allocated to the detection of disinformation	–	↓	–	–	↑	↑	–	50
Technology gap	Increasing R&D investment and financial support for start-ups, and scaling up companies related to digital technologies	–	–	–	↓	↓	↑	↑	50
Proactive approach	Improving diplomatic relations with countries considered strategic challenges	↑	↓	↑	↓	↓	–	–	48
Proactive approach	Creation of an EU news agency to ensure veracity of information	–	↓	↑	↓	↓	↑	–	46
Proactive approach	Mandatory creation of StratCom units at the highest level in EU countries and institutions	–	↓	↑	↓	↓	↑	↓	42
Coordination	Increasing operational intelligence capability at the EU level	–	↓	–	↓	–	↑	–	40

REFERENCES

AAUP. (2014). *On Partnerships with Foreign Governments: The Case of Confucius Institutes*. American Association of University Professors. https://www.aaup.org/file/Confucius_Institutes_0.pdf

Abellán, L. (2019, March 11). *El Gobierno activa una unidad contra la desinformación ante las elecciones*. El País. https://elpais.com/politica/2019/03/10/actualidad/1552243571_703630.html

Acosta, J. (2014, March). *U.S., other powers kick Russia out of G8*. CNN. https://www.cnn.com/2014/03/24/politics/obama-europe-trip/index.html

Adamsky, D. (2019). *Russian Nuclear Orthodoxy: Religion, Politics, and Strategy*. Stanford University Press.

AFP. (2017, September). *Russia's joint military exercise with Belarus rattles NATO; Moscow claims drills 'strictly defensive'*. World News - Firstpost. https://www.firstpost.com/world/russias-joint-military-exercise-with-belarus-rattles-nato-moscow-claims-drills-strictly-defensive-4044143.html

Afzal, M. (2019). *Saudi Arabia's hold on Pakistan* [Policy Brief]. Brookings. https://www.brookings.edu/wp-content/uploads/2019/05/FP_20190510_saudi_pakistan_afzal.pdf

Agence France Presse. (2018, September 15). *German Troops Face Russian 'Hybrid War' in Lithuania: Merkel | Military.com*. Military.Com. https://www.military.com/daily-news/2018/09/15/german-troops-face-russian-hybrid-war-lithuania-merkel.html

Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). *The state of deepfakes. Landscape, threats and impact*. Deeptrace. https://deeptracelabs.com/resources/

Alandete, D. (2017a, October). *Putin alienta la independencia con un enviado a Cataluña*. El País. https://elpais.com/politica/2017/10/25/actualidad/1508958307_955473.html

Alandete, D. (2017b, November 10). *European Union fights the Kremlin's propaganda machine*. El País. https://english.elpais.com/elpais/2017/11/09/inenglish/1510218067_521677.html

Alandete, D. (2017c, November 20). *El Centro de Comunicación Estratégica de la OTAN pide a España que se proteja ante la injerencia rusa*. El País. https://elpais.com/politica/2017/11/19/actualidad/1511112485_977295.html?rel=mas

Alandete, D. (2019). *Fake news: La nueva arma de destrucción masiva. Cómo se utilizan las noticias falsas y los hechos alternativos para desestabilizar la democracia*. Deusto.

Aleksa, C., Kuprienė, P., & Keršytė, L. (2016). *What we need to know about resistance. Active Guidelines*. Ministry of National Defense of the Republic of Lithuania.

Allen Institute for AI. (2019). *Grover—A State-of-the-Art Defense against Neural Fake News*. https://grover.allenai.org/

Allison, R. (2014, November). Russian 'deniable' intervention in Ukraine: How and why Russia broke the rules. *International Affairs*, *90*(6), 1255–1297. https://onlinelibrary.wiley.com/doi/10.1111/1468-2346.12170

Altay, I. (2019, December 20). *Cooperation with Malaysia, Qatar, Iran will continue, Erdoğan says*. Daily Sabah. https://www.dailysabah.com/diplomacy/2019/12/20/cooperation-with-malaysia-qatar-iran-will-continue-erdogan-says

Álvarez, G. (2014). *Los factores de riesgo económico en la crisis de Ucrania* (No. 32/2014). Instituto Español de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO32-2014_Ucrania_GregorioAlvarez.pdf

Alvargonzález, A. (2018, May 18). *NATO Deputy Secretary General Presentation*. Hybrid Warfare; New Threats, Spain Senate.

American Association of Universities. (2019). *Actions Taken by Universities to Address Growing Concerns about Security Threats and Undue Foreign Influence on Campus*. https://www.aau.edu/sites/default/files/Blind-Links/Effective-Science-Security-Practices.pdf

Andriukaitis, L. (2018). *Lisa's Case Repeated: German Soldiers Accused of Rape*. Vilniaus politikos analizės institutas. https://vilniusinstitute.lt/en/lisas-case-repeated-german-soldiers-accused-of-rape/

AOAV. (2017, May). *'Soft power' financing of religious, cultural and educational networks that nurture the jihadi ideology: Mosques and Islamic centres in the West*. https://aoav.org.uk/2017/soft-power-financing-religious-cultural-educational-networks-nurture-jihadi-ideology-mosques-islamic-centres-west/

Arnhold, N., Ziegele, F., & Kivistö, J. (2020, June). Under pressure: Covid-19 and the funding of European higher education. *World Bank Blogs*. https://blogs.worldbank.org/education/under-pressure-Covid-19-and-funding-european-higher-education

Atomico. (2020). *The state of European tech*. https://2019.stateofeuropeantech.com/

Atwood, K., & Klein, B. (2019, August). *G7 2020: Trump and Macron agree that Russia should be invited to conference*. CNNPolitics. https://edition.cnn.com/2019/08/20/politics/donald-trump-russia-g8-g7/index.html

Baezner, M. (2018). *Cyber and Information warfare in the Ukrainian conflict*. Center for Security Studies (CSS), ETH. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf

Bajarūnas, E., & Keršanskas, V. (2018). Hybrid Threats: Analysis of content, challenges posed and measures to overcome. *Lithuanian Annual Strategic Review*, *16*(1), 123–171. https://content.sciendo.com/configurable/contentpage/journals$002flasr$002f16$002f1$002farticle-p123.xml

Baltic News Service. (2019, December 16). *German troops taught to resist cyber attacks in Lithuania*. Lithuanian Radio and Television (LRT). https://www.lrt.lt/en/news-in-english/19/1125722/german-troops-taught-to-resist-cyber-attacks-in-lithuania

Baños, P. (2011, April). *Comunicación Estratégica. La clave de la victoria en el siglo XXI*. XVIII Curso Internacional de Defensa "Medios de Comunicación y Operaciones Militares".

Baqués, J. (2018). *Análisis de tendencias geopolíticas a escala global* (DIEEEINV18/2017). Instituto Español de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/docs_investig/2018/DIEEEINV18-2017_Analisis_Tendencias_Geopoliticas_EscalaGlobal_JosepBaques.pdf

BBC. (2015, April 10). *Yemen conflict: Pakistan rebuffs Saudi coalition call*. BBC News. https://www.bbc.com/news/world-asia-32246547

BBC. (2019, February). *Saudi Arabia signs $20bn in deals with Pakistan*. https://www.bbc.com/news/business-47274672

Bebler, A. (2015). *The Russian-Ukrainian conflict over Crimea*. International Institute for Middle East and Balkan Studies. https://www.ifimes.org/en/9035

Bennhold, K., & Ewing, J. (2020, January). *In Huawei battle, China threatens Germany 'Where it hurts': Automakers*. The New York Times. https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html

Bentzen, N. (2019). *The sharp power of knowledge: Foreign authoritarian meddling in academia*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/644207/EPRS_ATA(2019)644207_EN.pdf

Berbell, C. (2019, April). *Sólo hubo 5 heridos graves en el referéndum de 1 de octubre, según el exdirector de CatSalud*. Confilegal. https://confilegal.com/20190430-solo-hubo-5-heridos-graves-en-el-referendum-de-1-de-octubre-segun-el-exdirector-de-catsalud/

Bertholee, R. (2014, December). *Jihadism on the Rise in Europe: The Dutch Perspective—The Washington Institute for Near East Policy*. https://www.washingtoninstitute.org/policy-analysis/view/jihadism-on-the-rise-in-europe-the-dutch-perspective

Biswas, A., & Tortajada, C. (2018, February 23). *China's soft power is on the rise*. China Daily. http://www.chinadaily.com.cn/a/201802/23/WS5a8f59a9a3106e7dcc13d7b8.html

Bokhari, F., Politi, J., & Raval, A. (2018, October). *Saudi Arabia agrees to give $6bn financial support for Pakistan*. Financial Times. https://www.ft.com/content/18549b9c-d6e0-11e8-ab8e-6be0dcf18713

Bradshaw, J., & Freeze, C. (2013, February 7). *McMaster closing Confucius Institute over hiring issues*. The Globe and Mail. https://www.theglobeandmail.com/news/national/education/mcmaster-closing-confucius-institute-over-hiring-issues/article8372894/

Bradshaw, S., & Howard, P. (2019). *The global disinformation order. 2019 global inventory of organised social media manipulation* (Working Paper 2019.2). Oxford Internet Institute. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Briançon, P. (2020, March). *How Mario Draghi's 'Whatever it takes' became Europe's antivirus mantra*. MarketWatch. https://www.marketwatch.com/story/how-mario-draghis-whatever-it-takes-became-europes-antivirus-mantra-2020-03-20

Brookings. (2005). *China's Peaceful Rise: Speeches of Zheng Bijian 1997-2004*. Brookings. https://www.brookings.edu/wp-content/uploads/2012/04/20050616bijianlunch.pdf

Bughin, J., Seong, J., Manyika, J., Hämäläinen, L., Windhagen, E., & Hazan, E. (2019). *Notes from the AI frontier. Tackling Europe's gap in digital and AI*. McKinsey Global Institute. https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Tackling%20Europes%20gap%20in%20digital%20and%20AI/MGI-Tackling-Europes-gap-in-digital-and-AI-Feb-2019-vF.ashx

Buluc, R. (2018). Critical Thinking in the fight against fake news. *Mediating Globalisation: Identities in Dialogue*. https://www.researchgate.net/publication/326573452_Critical_Thinking_in_the_Fight_against_Fake_News

Canadian Heritage. (2019, July 2). Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation. *Government of Canada*. https://www.canada.ca/en/canadian-heritage/news/2019/07/helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html

CAUT. (2014). *Canadian campuses urged to end ties with Confucius Institutes*. Canadian Association of University Teachers. https://bulletin-archives.caut.ca/bulletin/articles/2014/01/canadian-campuses-urged-to-end-ties-with-confucius-institutes

Cavazos, R. (2019). *The economic cost of bad actors on the Internet: Fake news*. CHEQ & University of Baltimore. https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf

CCN-CERT. (2018). *Ciberamenazas y Tendencias Edición 2018* (CCN-CERT IA-09/18). Centro Criptológico Nacional. https://www.ccn-cert.cni.es/en/reports/public/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html

Cederberg, G. (2018). *Catching Swedish Phish—How Sweden is Protecting its 2018 elections*. Harvard Kennedy School - Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

Cembrero, I. (2017, October). *Consulta catalana 1-O: Ni siquiera Andorra: Solo Maduro y Kosovo dudan si reconocer la república catalana*. El Confidencial. https://www.elconfidencial.com/espana/2017-10-25/independencia-cataluna-maduro-kosovo_1466357/

Center for European Policy Analysis. (2017). *Combined Strategic Command-Staff Exercise (CSCSE) of Armed Forces of Belarus and Russia 'Zapad-2017'*. https://cepa.ecms.pl/files/?id_plik=4118

Center for Information Technology and Society - University California Santa Barbara. (2019). *How is fake news spread? Bots, people like you, trolls, and microtargeting*. https://www.cits.ucsb.edu/fake-news/spread

Center for International Security and Cooperation - Stanford University. (2019). *Islamic State*. https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state#text_block_18356

Centre d'Estudis d'Opinió. (2020). *Barómetro de opinión política 1ª ola 2020*. Generalitat de Catalunya. http://upceo.ceo.gencat.cat/wsceop/7548/Resumen%20en%20espa%C3%B1ol%20-962.pdf

CERT-EU. (2019). *RFC 2350*. https://cert.europa.eu/static/RFC2350/RFC2350.pdf

Cerulus, L. (2020, May). *How anti-5G anger sparked a wave of arson attacks*. Politico.Eu. https://www.politico.eu/article/coronavirus-5g-arson-attacks-online-theories/

Chatzky, A., & McBride J. (2020). *China's Massive Belt and Road Initiative*. Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

Cheo, J. (2018, April). *Fake news can make—Or break—Stock prices*. The Business Times. https://www.businesstimes.com.sg/opinion/fake-news-can-make-or-break-stock-prices

China Daily. (2006, May 29). *'China threat' fear countered by culture*. China Daily. http://www.chinadaily.com.cn/china/2006-05/29/content_602226.htm

Confucius Institute. (n.d.). *Constitution and By-Laws of the Confucius Institutes*. Confucius Institute. Retrieved 19 February 2020, from http://english.hanban.org/node_7880.htm

Conley, H., Rathke, J., & Melino, M. (2018). *Enhanced Deterrence in the North: A 21st Century European Engagement Strategy* (CSIS Europe Program). Center for Strategic and International Studies. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180119_Conley_EnhancedDeterrenceNorth_Web.pdf?uIa_1usRa2.PdrR4pnJvjLKFPN3tFDYQ

Cornish, P., Lindley-French, J., & Yorke, C. (2011). *Strategic communications and national strategy*. Chatham House. https://www.chathamhouse.org/sites/default/files/r0911es%E2%80%93stratcomms.pdf

Cottiero, C., Kucharski, K., Olimpieva, E., & Orttung, R. W. (2015). War of words: The impact of Russian state television on the Russian Internet. *Nationalities Papers*, *43*(4). https://doi.org/p

Council of the European Union. (2016). *Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization* (No. 15283/16). http://data.consilium.europa.eu/doc/document/ST-15283-2016-INIT/en/pdf

Council on Foreign Relations. (2020). *Conflict in Ukraine*. Global Conflict Tracker. https://cfr.org/interactive/global-conflict-tracker/conflict/conflict-ukraine

Counter Extremism Project. (2019). *The Netherlands: Extremism & Counter-Extremism*. https://www.counterextremism.com/countries/netherlands

Coyer, P. (2016). *The Patriarch, The Pope, Ukraine And The Disintegration Of 'The Russian World'*. Forbes. https://www.forbes.com/sites/paulcoyer/2016/03/20/the-patriarch-the-pope-ukraine-and-the-disintegration-of-the-russian-world/#10471ebd2523

Cubeiro, E. (2018). *Hybrid Warfare and Cyberspace*. 2018 Cyber Defence Conference, Spain. https://jornadasciberdefensa.es/documents/22_05_00_Conferencia_Guerra_hibrida_y_ciberespacio.pdf

Cybercrime Convention Committee (T-CY). (2019). *Aspects of election interference by means of computer systems covered by the Budapest Convention* (Guidance Note No. 9). Council of Europe. https://rm.coe.int/t-cy-2019-4-guidance-note-election-interference/1680965e23

Dalla Mora, M. (2019). *From the Euromaidan to the Hybrid War in the Donbass: An Analysis of the Ukraine Crisis and the Determinants of Russian Foreign Policy* (AV Akademikerverlag).

Damhuis, K. (2019). *"The biggest problem in the Netherlands": Understanding the Party for Freedom's politicization of Islam*. Brookings. https://www.brookings.edu/research/the-biggest-problem-in-the-netherlands-understanding-the-party-for-freedoms-politicization-of-islam/

Darczewska, J. (2017). *Putin's Cossacks, Folklore, Business or Politics?* Center for Eastern Studies. https://www.osw.waw.pl/sites/default/files/pw_68_putin_cossacks_net_0.pdf

Davis, J. R. (2015). Continued evolution of hybrid threats. The Russian hybrid threat construct and the need for innovation. *The Three Swords Magazine*, *28*, 19–25. http://www.jwc.nato.int/images/stories/threeswords/JWC_Magazine_May2015_web_low.pdf

Dawn.com. (2015, April 11). *UAE minister warns Pakistan of 'heavy price for ambiguous stand' on Yemen—Pakistan*. Dawn - World. https://www.dawn.com/news/1175284

Debunk. (n.d.). *About DEBUNK* [Debunk.eu]. Retrieved 12 March 2020, from https://debunk.eu/

del Castillo, I. (2019, December). *Telefónica contrata a Huawei una parte de su red de 5G en España*. Expansión. https://www.expansion.com/empresas/tecnologia/2019/12/06/5de9788e468aebe15a8b45fb.html

Department of Home Affairs. (2019a, August 19). National Counter Foreign Interference Coordinator. *Australian Government*. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-coordinator#

Department of Home Affairs. (2019b, August 29). *Australia's Counter Foreign Interference Strategy*. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-strategy

Diena. (2017, October 8). *Broadcast: The mobile interference observed in Kurzeme may have been caused by a Russian device*. Diena.lv. https://www.diena.lv/raksts/latvija/zinas/raidijums-kurzeme-noverotos-mobilo-sakaru-traucejumus-iespejams-radijusi-krievijas-ierice-14182244

Digitalle Gesellschaft. (2017). *Declaration on freedom of expression*. http://deklaration-fuer-meinungsfreiheit.de/en/

disinfo.eu. (2020, March). *Disinformation can kill*. EU vs DISINFORMATION. https://euvsdisinfo.eu/disinformation-can-kill/

Draghi, M. (2012, July 26). *Verbatim of the remarks made by the President of European Central Bank, Mario Draghi—Speech at the Global Investment Conference in London*. European Central Bank. https://www.ecb.europa.eu/press/key/date/2012/html/sp120726.en.html

Driscoll, J., & Steinert-Threlkeld, Z. (2020). Social media and Russian territorial irredentism: Some facts and a conjecture. *Post-Soviet Affairs*, *36*(2), 101–121. https://www.tandfonline.com/doi/full/10.1080/1060586X.2019.1701879

Dutch Safety Board. (2015). *MH17 Crash*. https://www.onderzoeksraad.nl/en/media/attachment/2018/7/10/debcd724fe7breport_mh17_crash.pdf

DW. (2017, February 17). *Lithuanian authorities launch investigation into fake German rape story*. Deutsche Welle (DW). https://www.dw.com/en/lithuanian-authorities-launch-investigation-into-fake-german-rape-story/a-37608180

EACS. (2014, July 30). *Letter of Protest at Interference in EACS Conference in Portugal, July 2014*. European Association for Chinese Studies. http://chinesestudies.eu/?p=585

East StratCom Task Force. (2018). Ukrainian Church's demand for autocephaly is a CIA special operation, not a religious conflict or a split. *EU vs DISINFORMATION*. https://euvsdisinfo.eu/report/ukrainian-churchs-demand-for-autocephaly-is-a-cia-special-operation-not-a-religious-conflict-ora-split/

East StratCom Task Force. (2019a, September). *Disinfo: JIT conclusions on the downing of MH17 are not objective* -. EU vs DISINFORMATION. https://euvsdisinfo.eu/report/jit-conclusions-on-the-downing-of-mh17-are-not-objective/

East StratCom Task Force. (2019b, October 31). Attacking Ukrainian church: The Kremlin turns the Orthodox world into a battlefield. *Euromaidan Press*. http://euromaidanpress.com/2019/10/31/attacking-ukrainian-church-the-kremlin-turns-the-orthodox-world-into-a-battlefield/

East StratCom Team. (2015). *Action Plan on Strategic Communication* (Ref. Ares(2015)2608242). http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf

Ekholm, B. (2019, December). *The real reason Europe is falling behind in 5G*. Ericsson. https://www.ericsson.com/en/blog/2019/12/Borje-Ekholm-5G-Europe-falling-behind

Elcano Royal Institute. (2018). *The conflict in Catalonia*. http://www.realinstitutoelcano.org/wps/wcm/connect/c0f90dae-76d1-4a8e-8f78-0058f048a44b/Catalonia-Dossier-Elcano-October-2017.pdf?MOD=AJPERES&CACHEID=c0f90dae-76d1-4a8e-8f78-0058f048a44b

Emmott, R. (2017, October). *NATO says Russia misled West over scale of Zapad war games*. Reuters. https://www.reuters.com/article/us-nato-russia/nato-says-russia-misled-west-over-scale-of-zapad-war-games-idUSKBN1CV2K4

ENISA. (2016). *Threat Taxonomy*. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/at_download/file

ENISA. (2017). *Baseline security recommendations for IoT in the context of critical information infrastructures*. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

ENISA. (2019). *CONSULTATION PAPER - EU ICT INDUSTRIAL POLICY: BREAKING THE CYCLE OF FAILURE*. ENISA. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper

EPRS. (2015). *At a glance: Understanding hybrid threats*. http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf

EPRS. (2018). *Foreign influence operations in the EU* [Briefing]. European Parliament Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf

Ericsson. (2019). *Ericsson Mobility Report*. https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf

Esteban, M. (2016). *The new drivers of Asia's global presence* (ARI 9/2016). Royal Institute Elcano. http://www.realinstitutoelcano.org/wps/wcm/connect/605105804b648beaae83bfeeaa369edc/ARI9-2016-Esteban-New-drivers-Asia-global-presence.pdf?MOD=AJPERES&CACHEID=605105804b648beaae83bfeeaa369edc

Esteban, M. (2017). *The foreign policy of Xi Jinping after the 19th Congress: China strives for a central role on the world stage* (ARI 87/2017). Royal Institute Elcano. http://www.realinstitutoelcano.org/wps/wcm/connect/cf3c30c6-a9c5-4524-b099-57fa42e2bc7a/ARI87-2017-Esteban-Foreign-policy-Xi-Jinping-19th-Congress-China-central-role-world-stage.pdf?MOD=AJPERES&CACHEID=cf3c30c6-a9c5-4524-b099-57fa42e2bc7a

ETSI. (2019). *ETSI - Mobile Technologies—5g, 5g Specs | Future Technology*. https://www.etsi.org/technologies/5g

Euroactiv. (2018). *Migration and security in Europe: Is immigration a threat or an asset?* https://en.euractiv.eu/wp-content/uploads/sites/2/special-report/EURACTIV-Special-Report-Migration-and-security-in-Europe.pdf

Eurobarometer. (2019). *Public opinion in the European Union* (Standard Eurobarometer No. 92). https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/88848

European Commission. (2013). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

European Commission. (2014a). *Communication from the Commission to the European Parliamentmthe Council, the European Economic and Social Committee and the Committiee of the Regions—For a European Industrial Renaissance* (COM(2014) 14 final). European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0014&from=EN

European Commission. (2014b, March). *European Commission's support to Ukraine*. European Commission - Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/IP_14_219

European Commission. (2016a). *Joint communication to the European Parliament and the Council: Joint Framework on countering hybrid threats, a European Union Response* (JOIN(2016) 18 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

European Commission. (2016b). *Joint Staff Working Document EU operational protocol for countering hybrid threats 'EU Playbook'* (No. 11034/16). http://statewatch.org/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf

European Commission. (2017a). *Joint Communication to the European Parliament and th Council—A Strategic Approach to Resilience in the EU's external action* (JOIN(2017) 21 final). https://eeas.europa.eu/sites/eeas/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf

European Commission. (2017b). *Joint Communication to the European Parliament and the Council—Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (JOIN(2017) 450 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

European Commission. (2018a). *Synopsis report of the public consultation on fake news and online disinformation*. https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-fake-news-and-online-disinformation

European Commission. (2018b). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation: A European Approach* (COM(2018) 236 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN

European Commission. (2018c). *Fake news and disinformation online* (Flash Eurobarometer No. 464). https://data.europa.eu/euodp/en/data/dataset/S2183_464_ENG

European Commission. (2018d). *Artificial Intelligence for Europe* (Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2018) 237). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN

European Commission. (2018e). *Joint Communication to the European Parliament, the European Council and the Council—Increasing resilience and bolstering capabilities to address hybrid threats* [JOIN(2018) 16 final]. https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf

European Commission. (2018f). *Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online* (Commission Staff Working Document SWD(2018) 408 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0408&from=EN

European Commission. (2018g, September 12). *State of the Union 2018: European Commission proposes measures for securing free and fair European elections*. European Commission - Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681

European Commission. (2018h). *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions—Action Plan against Disinformation* (JOIN(2018) 36 final). https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf

European Commission. (2018i). *Coordinated Plan on Artificial Intelligence* (Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2018) 795). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56018

European Commission. (2019a). *Media literacy*. Shaping Europe's Digital Future. https://ec.europa.eu/digital-single-market/en/media-literacy

European Commission. (2019b, June). *Code of Practice on Disinformation | Digital Single Market*. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

European Commission. (2019c). *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions—Report on the implementation of the Action Plan Against Disinformation* (JOIN(2019) 12 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

European Commission. (2019d, September). *Tackling online disinformation | Shaping Europe's digital future*. https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

European Commission. (2020a). *2018 – 2019 Call for proposals for Preparatory Action on Media Literacy for All*. Shaping Europe's Digital Future. https://ec.europa.eu/digital-single-market/en/news/2018-2019-call-proposals-preparatory-action-media-literacy-all

European Commission. (2020b). *Secure 5G deployment in the EU - Implementing the EU toolbox* (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2020) 50 final). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64481

European Commission. (2020c). *White paper On Artificial Intelligence—A European approach to excellence and trust* (COM(2020) 65 final). https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Commission. (2020d). *Attitudes towards the impact of digitalisation on daily lives* (Special Eurobarometer No. 503). https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/89800

European Commission. (2020e). *European Civil protection and humanitarian aid operations: Ukraine*. https://ec.europa.eu/echo/where/europe/ukraine_en#:~:text=Since%202014%2C%20the%20European%20Union,humanitarian%20and%20early%20recovery%20aid.&text=The%20EU%20is%20one%20of,13%20million%20allocated%20in%202020

European Commission. (2020f, June). *The Digital Services Act package*. Shaping Europe's Digital Future. https://ec.europa.eu/digital-single-market/en/digital-services-act-package

European Commission and the High Representative. (2019). *EU-China – A strategic outlook*. https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf

European Commission and the High Representative. (2020). *Tackling Covid-19 disinformation—Getting the facts right*. https://ec.europa.eu/info/sites/info/files/communication-tackling-Covid-19-disinformation-getting-facts-right_en.pdf

European Council. (2014). *EU human rights guidelines on freedom of expression online and offline*. https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf

European Council. (2015). *European Council meeting (19 and 20 March 2015)—Conclusions* (EUCO 11/15). https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

European Council. (2018a). *European Council conclusions on the Salisbury attack*. European Council - Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2018/03/22/european-council-conclusions-on-the-salisbury-attack/

European Council. (2018b). *Council recommendation of 22 May 2018 on key competences for lifelong learning* (2018/C 189/01). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0604(01)&from=es

European Council. (2018c). *European Council meeting (28 June 2018)—Conclusions* (EUCO 9/18). https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf

European Council. (2018d). *EU HEX-ML 18 (PACE): European Union hybrid exercise multilayer 18 (parallel and coordinated exercise)*. https://data.consilium.europa.eu/doc/document/ST-13577-2018-INIT/en/pdf

European Council. (2019a). *Non paper on attribution of malicious cyber activities in the context of the framework for a joint EU diplomatic response to malicious cyber activities*. http://www.statewatch.org/news/2019/mar/eu-council-cyber-6852-REV-1-19.pdf

European Council. (2019b). *Complementary efforts to enhance resilience and counter hybrid threats—Council conclusions (10 December 2019)* (No. 14972/19). Council of the European Union. https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf

European Council. (2020a). *EU restrictive measures in response to the crisis in Ukraine*. http://www.consilium.europa.eu/en/policies/sanctions/ukraine-crisis/

European Council. (2020b, March). *Sanctions: How and when the EU adopts restrictive measures*. Policies. https://www.consilium.europa.eu/en/policies/sanctions/

European Court of Auditors. (2019). *Challenges to effective EU cybersecurity policy*. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

European Court of Auditors. (2020). *Audit preview—Action Plan Against Disinformation*. European Court of Auditors. https://www.eca.europa.eu/lists/ecadocuments/ap20_04/ap_disinformation_en.pdf

European External Action Service. (2016a). *Shared vision, common action: A stronger Europe. A global strategy for the European Union's foreign and security policy*. https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf

European External Action Service. (2016b). *A Global Strategy for the European Union's Foreign And Security Policy*. https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf

European External Action Service. (2020, June). *EU-China Strategic Dialogue: Remarks by High Representative/Vice-President Josep Borrell at the press conference*. EEAS Homepage. https://eeas.europa.eu/headquarters/headquarters-homepage/80639/eu-china-strategic-dialogue-remarks-high-representativevice-president-josep-borrell-press_en

European Journalists Association. (2017). *XXIX Seminario Internacional de Seguridad y Defensa. ¿Hacia un nuevo (des)orden mundial?* http://www.apeuropeos.org/xxix-seminario-internacional-de-seguridad-y-defensa-hacia-un-nuevo-desorden-mundial/

European Parliament. (2016a). *European Parliament resolution of 4 February 2016 on the human rights situation in Crimea, in particular of the Crimean Tatars*.

European Parliament. (2016b). *European Parliament resolution of 12 May 2016 on the Crimean Tatars*. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0218_EN.html?redirect

European Parliament. (2016c). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* (L 194/1). https://eur-lex.europa.eu/eli/dir/2016/1148/oj

European Parliament. (2016d). *European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties* (P8_TA(2016)0441). http://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.pdf

European Parliament. (2017a). *European Parliament legislative resolution of 6 April 2017 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 539/2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (Ukraine)*. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0129_EN.html?redirect

European Parliament. (2017b). *European Parliament resolution of 16 March 2017 on the Ukrainian prisoners in Russia and the situation in Crimea*. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0087_EN.html?redirect

European Parliament. (2018a). *European Parliament resolution of 12 December 2018 on the implementation of the EU Association Agreement with Ukraine*. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0518_EN.html?redirect

European Parliament. (2018b). *Defence of academic freedom in the EU's external action*. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0483_EN.pdf

European Parliament. (2019). *European Parliament recommendation of 13 March 2019 to the Council and the Vicepresident of the Commission / High Follow up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties (2018/2115(INI))* (P8_TA(2019)0187). https://www.europarl.europa.eu/doceo/document/TA-8-2019-0187_EN.pdf

European Parliament. (2020). *EU coordinated action to combat the Covid-19 pandemic and its consequences* (European Parliament Resolution P9_TA(2020)0054). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf

European Parliament and the Council. (2000). *Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

European Union Agency for Fundamental Rights. (2017). *Second European Union Minorities and Discrimination Survey. Muslims – Selected findings*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-eu-minorities-survey-muslims-selected-findings_en.pdf

European Union Institute for Security Studies. (2016). *EU strategic communications with a view to counteracting propaganda*. European Parliament. http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf

Europol. (2018). *Internet organised crime threat assessment 2018*. https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

Eurostat. (2020). *Individuals' level of digital skills*.

Executive Officer of the President. (2019). *Securing the information and communications technology and services supply chain* (Executive Order No. 13873). https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf

FactBar EDU. (2018). *Elections approach – are you ready? Fact-checking for educators and future voters*. https://www.faktabaari.fi/assets/FactBar_EDU_Fact-checking_for_educators_and_future_voters_13112018.pdf

Fägersten, B. (2016). *For EU eyes only? Intelligence and European security* (Brief Issue No. 8–2016). European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_8_EU_Intelligence_Cooperation.pdf

Fine, S. (2019). *All at sea: Europe's crisis of solidarity on migration*. European Council on Foreign Relations. https://www.ecfr.eu/page/-/all_at_sea_europes_crisis_of_solidarity_on_migration.pdf

Fiott, D., & Parkes, R. (2019). *The EU's response to hybrid threats* (Chaillot Paper No. 151). EU Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

Flanagan, S., Osburg, J., Binnendijk, A., Kepe, M., & Radin, A. (2019). *Deterring Russian aggression in the Baltic States through resilience and resistance*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2779.html

Foster, P., & Holehouse, M. (2016, January 16). *Russia accused of clandestine funding of European parties as US conducts major review of Vladimir Putin's strategy*. The Telegraph. https://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html

G7. (2018). *Charlevoix Commitment on Defending Democracy from Foreign Threats*. https://www.mofa.go.jp/files/000373846.pdf

Galán, C. (2019, September 11). Certification as a control mechanism of Artificial Intelligence in Europe. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3451741

García-Muñoz, C. (2018). Achievements and limits of strategic communication for nation-building: The case of Spain's Catalan region (1979-2017). *Revista Internacional de Relaciones Públicas*, *VIII*(15), 129–152. https://dialnet.unirioja.es/descarga/articulo/6488996.pdf

General Intelligence and Security Service. (2005). *Saudi influences in the Netherlands. Links between the Salafist mission, radicalisation processes and Islamic terrorism*. https://english.aivd.nl/binaries/aivd-en/documents/publications/2005/01/06/saudi-influences-in-the-netherlands/saudiinfluencesinthenetherlands.pdf

General Intelligence and Security Service. (2010). *Resilience and Resistance. Current trends and developments in Salafism in the Netherlands*. Government of the Netherlands. https://english.aivd.nl/binaries/aivd-en/documents/publications/2010/04/14/resilience-and-resistance/resilienceandresistancedefpfdeng.pdf

General Intelligence and Security Service. (2015). *Salafism in the Netherlands: Diversity and dynamics*. Government of the Netherlands. https://english.aivd.nl/binaries/aivd-en/documents/publications/2015/09/24/salafism-in-the-netherlands-diversity-and-dynamics/salafism-in-the-netherlands.pdf

General Intelligence and Security Service. (2018). *Syria's Legacy. Global jihadism remains a threat to Europe*. Government of the Netherlands. https://english.aivd.nl/binaries/aivd-en/documents/publications/2018/11/09/the-legacy-of-syria-global-jihadism-remains-a-threat-to-europe/Legacy+of+Syria+-+Global+jihadism+remains+a+threat+to+Europe.pdf

General Intelligence and Security Service. (2019). *AIVD Annual Report 2018*. Ministry of the Interior and Kingdom Relations - Government of the Netherlands. https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2019/05/14/aivd-annual-report-2018/AIVD+Annual+Report+2018.pdf

Gerasimov, V. (2013, February). The value of science is in the foresight. New challenges demand rethinking the forms and methods of carrying out combat operations. *Military-Industrial Kurier*. https://jmc.msu.edu/50th/download/21-conflict.pdf

Gibson, K. H. (2019, September). *Lessons learned from NATO's hybrid battlefield* [Panel]. Defence News Conference.

Gil, T. (2020, March 18). *Coronavirus: Cómo el virus se volvió parte de la 'guerra' política entre EE.UU. y China*. BBC News Mundo. https://www.bbc.com/mundo/noticias-internacional-51938799

Global Spain. (2018). *Who we are | #ThisIsTheRealSpain*. https://www.thisistherealspain.com/en/quienes-somos/

Global Spain. (2019a). *Spain: A global actor in the fight against climate change*. https://www.thisistherealspain.com/wp-content/uploads/2019/11/DOSIER-COP25-INGL%C3%89S_web.pdf

Global Spain. (2019b). *The truth about Catalonia's bid for independence*. https://www.thisistherealspain.com/wp-content/uploads/2019/11/THE-TRUTH-ABOUT-THE-CATALAN-INDEPENDENCE-BID-28-nov-2019.pdf

Global Spain. (2019c). *Information about the Catalan independence bid*. https://www.thisistherealspain.com/wp-content/uploads/2019/09/THE-TRUTH-ABOUT-THE-CATALAN-INDEPENDENCE-BID.pdf

GlobalFirePower. (2020). *GFP power ranking index of nations since 2005*. https://www.globalfirepower.com/global-ranks-previous.asp

Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones., BOE-A-2019-15790 20 (2019). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-15790

Goldman, E. (2007). Strategic communication: A tool for asymmetric warfare. *Small Wars Journal*. https://smallwarsjournal.com/blog/strategic-communication-a-tool-for-asymmetric-warfare

Gotkowska, J. (2017, April 12). *The Cyber and Information Space: A new formation in the Bundeswehr*. Centre for Eastern Studies - OSW. https://www.osw.waw.pl/en/publikacje/analyses/2017-04-12/cyber-and-information-space-a-new-formation-bundeswehr

Government of Canada. (2019a, January). *G7 Rapid Response Mechanism*. https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html

Government of Canada. (2019b, July 9). Cabinet Directive on the Critical Election Incident Public Protocol. *Government of Canada*. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol/cabinet.html

Government of Canada. (2019c, August 30). *Online disinformation*. https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html#a2

Government of Spain. (2012). *Royal Decree 998/2012 of 28 June establishing the High Commission of the Government for the Spain Brand and amending Royal Decree 1412/2000 of 21 July establishing the Foreign Policy Council*. https://www.boe.es/boe/dias/2012/06/29/pdfs/BOE-A-2012-8672.pdf

Government of Spain. (2018). *Royal Decree 1266/2018 of 8 October amending Royal Decree 355/2018 of 6 June restructuring ministerial departments*. https://www.boe.es/boe/dias/2018/10/09/pdfs/BOE-A-2018-13715.pdf

Government of the Netherlands. (2014). *The Netherlands comprehensive action programme to combat jihadism. Overview of measures and actions*. https://data2.unhcr.org/en/documents/download/44369

Granville, K. (2018, March). *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*. The New York Times. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Gressel, G. (2019). *Protecting Europe against hybrid threats*. European Council on Foreign Relations. https://www.ecfr.eu/publications/summary/protecting_europe_against_hybrid_threats

Grieger, G. (2019). *5G in the EU and Chinese telecoms suppliers*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf

GSMA. (2019, February 14). *GSMA Calls on Europe to Safeguard Network Security and Competition in the Supply of Telecommunications Infrastructure*. Newsroom. https://www.gsma.com/newsroom/statement/gsma-calls-on-europe-to-safeguard-network-security/

Guilong, Y. (2019). *The impact of Artificial Intelligence on hybrid warfare* (DOI: 10.1080/09592318.2019.1682908). https://www.tandfonline.com/doi/abs/10.1080/09592318.2019.1682908

Hanlon, B., & Rosenberger, L. (2019). Countering Information Operations Demands A Common Democratic Strategy. *Alliance for Securing Democracy*. https://securingdemocracy.gmfus.org/countering-information-operations-demands-a-common-democratic-strategy/

Hansen, F., van der Noordaa, R., Bogen, O., & Sundbom, H. (2018). *The Kremlin's trojan horses. Russian influence in Denmark, The Netherlands, Norway and Sweden*. Atlantic Council. https://www.atlanticcouncil.org/publications/reports/the-kremlins-trojan-horses-3-0

Happold, M. (2016). *Economic sanctions and international law: An introduction*. Hart Publishing. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2837786

Heath, R. (2017, September). *Russia 'downright lying' about military exercises: Slovak ex-envoy*. POLITICO. https://www.politico.eu/article/zapad-russia-downright-lying-about-military-exercises-zapad-tomas-valasek-eu-confidential-belarus-estonia-latvia-lithuania/

Heidi T., & Leerssen, P. (2019). *An Analysis of Germany's NetzDG Law*. Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression. ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf

High Level Group on fake news and online disinformation- European Commission. (2018). *A multi-dimensional approach to disinformation—Report of the independent High Level Group on fake news and online disinformation* (doi:10.2759/739290). https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1

Hoffman, F. G. (2018). Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *PRISM - National Defense University*, *7*(4), 18. https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/

Holdert, M., & Kouwenhoven, A. (2018, April). *Geheime lijsten financiering moskeeën onthuld*. Nieuwsuur. https://nos.nl/nieuwsuur/artikel/2228686-geheime-lijsten-financiering-moskeeen-onthuld.html

Holroyd, M. (2019, June). *Why did Sea-Watch 3 decide to enter Italian territorial waters?* Euronews. https://www.euronews.com/2019/06/26/why-did-sea-watch-3-decide-to-enter-italian-territorial-waters

Hoorens, S., Krapels, J., Long, M., Keatinge, T., Van der Meulen, N., Kruithof, K., Bellasio, J., Psiaki, A., & Aliyev, G. (2015). *Foreign financing of Islamic institutions in the Netherlands*. RAND Europe. https://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR992/RAND_RR992.pdf

House of Commons. Foreign Affairs Committee. (2019). *A cautious embrace: Defending democracy in an age of autocracies*. https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/109.pdf

Huckle, S., & White, M. (2017). *Fake news: A technological approach to proving the origins of content, using blockchains*. University of Sussex.

https://www.researchgate.net/publication/321790598_Fake_News_A_Technological_Approach_to_Proving_the_Origins_of_Content_Using_Blockchains

Hybrid CoE. (2019). *Countering disinformation: News media and legal resilience* [COI Records]. European Centre of Excellence and the Media Pool, part of the Finnish Emergency Supply Organization in Helsinki. https://www.hybridcoe.fi/wp-content/uploads/2019/11/News-Media-and-Legal-Resilience_2019_rgb.pdf

Hybrid CoE. (2020a). *Hybrid threats—Hybrid CoE*. https://www.hybridcoe.fi/hybrid-threats/

Hybrid CoE. (2020b, June 25). *The Covid-19 crisis situation – a hybrid warfare perspective*. Hybrid CoE. https://www.hybridcoe.fi/news/the-Covid-19-crisis-situation-a-hybrid-warfare-perspective/

IDC. (2019, June 18). *The Growth in connected IoT devices is expected to generate 79.4ZB of data in 2025, according to a new IDC forecast*. IDC Media Center. https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Inspectorate for Security and Justice. (2017). *Evaluation of the Netherlands comprehensive action programme to combat jihadism*. Government of the Netherlands. https://www.inspectie-jenv.nl/binaries/inspectie-venj/documenten/rapporten/2017/09/06/evaluation-of-the-netherlands-comprehensive-action-programme-to-combat-jihadism/Evaluation+of+the+Netherlands+comprehensive+action+programme+to+combat+jihadism.pdf

Institute of Democracy and Cooperation. (2016). *Institut de la Democratie et de la Cooperation*. http://www.idc-europe.org/en/The-Institute-of-Democracy-and-Cooperation

Interfax-Ukraine. (2013, November 21). *Ukrainian government issues decree to suspend preparations for signing of association agreement with EU*. https://en.interfax.com.ua/news/general/176073.html

Isaac, M., & Alba, D. (2019, September 4). Big Tech Companies Meeting With U.S. Officials on 2020 Election Security. *The New York Times*. https://www.nytimes.com/2019/09/04/technology/2020-election-facebook-google.html

Janda, J. (2016). *The Lisa Case—STRATCOM Lessons for European states* (Security Policy Working Paper No. 11/2016). Federal Academy for Security Policy. https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf

Jintao, H. (2007, October 25). *Hu Jintao's report at 17th Party Congress*. China.Org.Cn. http://www.china.org.cn/english/congress/229611.htm#7

Johnson, D. (2018, December). VOSTOK 2018: Ten years of Russian strategic exercises and warfare preparation. *NATO Review*. https://www.nato.int/docu/review/articles/2018/12/20/vostok-2018-ten-years-of-russian-strategic-exercises-and-warfare-preparation/index.html

Jongbloed, B. (2018). Public Funding of Higher Education. In *Encyclopedia of International Higher Education Systems and Institutions* (Teixeira, P., Shin, J.). https://doi.org/10.1007/978-94-017-9553-1_74-1

Karnitschnig, M. (2020, March 18). *China is winning the coronavirus propaganda war*. POLITICO. https://www.politico.eu/article/coronavirus-china-winning-propaganda-war/

Kogan, S., Moskowitz, T., & Niesnner, M. (2019). *Fake News: Evidence from Financial Markets*. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3375153_code2148550.pdf?abstractid=3237763&mirid=1

Koren, S. (2019, July). *Introducing the News Provenance Project*. NYT Open. https://open.nytimes.com/introducing-the-news-provenance-project-723dbaf07c44

Krastev, I. (2005, October 19). *Russia's post-orange empire*. Open Democracy. https://www.opendemocracy.net/en/postorange_2947jsp/

Kremidas, C. (2019, November). *The vital role of public-private partnerships in countering hybrid threats*. Friends of Europe. https://www.friendsofeurope.org/insights/the-vital-role-of-public-private-partnerships-in-countering-hybrid-threats/

Krusten, M. (2019, November). *Fighting fake news with blockchain* [E-Estonia]. https://e-estonia.com/fighting-fake-news-with-blockchain/

Lackner, H. (2020). *Yemen: Why the Riyadh Agreement is collapsing*. European Council on Foreign Relations. https://www.ecfr.eu/article/commentary_yemen_why_the_riyadh_agreement_is_collapsing

Laity, M. (2018). NATO and Strategic Communications: 'The Story So Far'. *The Three Swords Magazine*, *33*, 65–73. http://www.jwc.nato.int/images/stories/threeswords/THREESWORDSMARCH2018_Websitereleased.pdf

Lannes, B. (1999). Propaganda. *Britannica*. https://www.britannica.com/topic/propaganda

Lasconjarias, G., & Dyčka, L. (2017). *Dealing with the Russian Bear: Improving NATO's Response to Moscow's Military Exercise Zapad 2017*. Istituto Affari Internazionali. https://www.iai.it/sites/default/files/iaicom1718.pdf

Laub, Z., & Robinson, K. (2020). *Yemen in crisis*. Council on Foreign Relations. https://www.cfr.org/backgrounder/yemen-crisis

Lázaro, A. (2014). *Ucrania, entre Rusia y Occidente* (UOC).

Lenoir-Grand, R. (2017, July 6). 'Enhanced Forward Presence', la respuesta disuasoria de la OTAN ante la amenaza rusa. *73/2017*. http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO73-2017_Respuesta_disuasoria_OTAN_Amenaza_Rusia_RicardoLenoir.pdf

Leonir-Grand, R. (2017). *Zapad 2017: Contexto, impacto y posibles consecuencias de los ejercicios militares rusos*. Instituto Español de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO102-2017_Zapad_Rusia_RicardoLenoir_Grand.pdf

Lesaca, J. (2017). *Why did Russian social media swarm the digital conversation about Catalan independence?* https://www.societatcivilcatalana.cat/sites/default/files/russian-social-media-intervention.pdf

Lessenski, M. (2018). *Common sense wanted. Resilience to 'post-truth' and its predictors in the new media literacy index 2018*. Open Society Institute. http://osi.bg/downloads/File/2018/MediaLiteracyIndex2018_publishENG.pdf

Luhn, A. (2015, September). *Russia funds Moscow conference for US, EU and Ukraine separatists*. The Guardian. https://www.theguardian.com/world/2015/sep/20/russia-funds-moscow-conference-us-eu-ukraine-separatists

Mahmood, F., & Ali, A. (2015, April 10). *Pakistan MPs draft resolution urging neutrality in Yemen crisis*. Reuters. https://www.reuters.com/article/us-yemen-security-pakistan/pakistan-mps-draft-resolution-urging-neutrality-in-yemen-crisis-idUSKBN0N10NP20150410

Marcin, M. (2016). Russia and its international image: From Sochi Olympic Games to annexing Crimea. *International Studies. Interdisciplinary Political and Cultural Journal*, *18*(2), 165–186. https://www.researchgate.net/publication/315823482_Russia_and_Its_International_Image_From_Sochi_Olympic_Games_to_Annexing_Crimea

Marcos, J. (2016, June). *Podemos: Venezuela Assembly probes Podemos funding from Chávez regime*. El País. https://elpais.com/elpais/2016/06/17/inenglish/1466151454_189201.html

Marsden, C., & Meyer, T. (2019). *Regulating disinformation with artificial intelligence*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf

Martens, B., Aguiar, L., Gómez-Herrera, E., & Mueller-Langer, F. (2018). *The Digital Transformation of News Media and the Rise of Disinformation and Fake News* (JRC Digital Economy Working Paper No. 2018–02). European Commission, Joint Research Centre. https://www.ssrn.com/abstract=3164170

Maslen, G. (2019, September). *Sharp fall in number of visas issued to Chinese students*. University World News. https://www.universityworldnews.com/post.php?story=20190925132954975

McKew, M. (2017). *The Gerasimov Doctrine*. POLITICO Magazine. https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538

Milosevich-Juaristi, M. (2017a). *Zapad-2017: Las maniobras militares rusas como ingrediente de la disuasión estratégica* (ARI 64/2017). Royal Instituto Elcano. http://www.realinstitutoelcano.org/wps/wcm/connect/3aaf1c78-3fe8-4245-b01b-a6ab449401f0/ARI64-2017-MilosevichJuaristi-Zapad-2017-maniobras-militares-Rusia-disuasion-estrategica.pdf?MOD=AJPERES&CACHEID=3aaf1c78-3fe8-4245-b01b-a6ab449401f0

Milosevich-Juaristi, M. (2017b). *La "combinación", instrumento de la guerra de la información de Rusia en Cataluña* (ARI 86/2017). Elcano Royal Institute. http://www.realinstitutoelcano.org/wps/wcm/connect/da86de12-7bb7-43cd-9b5e-72a4b8e9c351/ARI86-2017-MilosevichJuaristi-Combinacion-instrumento-guerra-informacion-Rusia-Cataluna.pdf?MOD=AJPERES&CACHEID=da86de12-7bb7-43cd-9b5e-72a4b8e9c351

Ministry of Awqaf & Islamic Affairs. (n.d.). *About the Ministry*. Retrieved 13 July 2020, from http://islam.gov.kw/Pages/en/AwqafDetails.aspx?id=7

Ministry of Defence of Georgia. (2017). *Strategic Defence Review 2017-2020* (p. 38). https://mod.gov.ge/uploads/2018/pdf/SDR-ENG.pdf

Ministry of Foreign Affairs. (2017, October). *Foreign Minister Dmitriy Medoev's Answers to Questions from TASS*. Ministry of Foreign Affairs - Republic of South Ossetia. http://www.mfa-rso.su/en/node/2347

Ministry of Foreign Affairs, European Union and Cooperation. (2018). *España Global*. Https://Www.Thisistherealspain.Com/En/. http://www.exteriores.gob.es/Portal/en/PoliticaExteriorCooperacion/MarcaEsp/Paginas/inicio.aspx

Ministry of National Defence of the Republic of Lithuania. (2017). *National Security Strategy*. Seimas of the Republic of Lithuania. https://kam.lt/en/defence_policy_1053/important_documents/strategical_documents.html

Ministry of national defence, & State security department of the Republic of Lithuania. (2020). *National threat assessment 2020*. https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-En.pdf

Ministry of Overseas Pakistanis & Human Resource Development. (2019). *Year Book 2017-2018*. Government of Pakistan. http://ophrd.gov.pk/SiteImage/Misc/files/Year-Book-2017-18.pdf

Ministry of the Presidency, Relations with the Courts and Democratic Memory. (2020). *Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional*. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-13663

Mueller, R. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. US Department of Justice. https://www.justice.gov/storage/report.pdf

National Coordinator for Security and Counterterrorism. (2019). *Terrorist Threat Assessment for the Netherlands 51*. Government of the Netherlands. https://english.nctv.nl/documents/publications/2019/12/19/terrorist-threat-assessment-netherlands-51

NATO. (2009a, April). *NATO - Official text: Strasbourg / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl*. https://www.nato.int/cps/en/natolive/news_52837.htm

NATO. (2009b). *NATO Strategic Communications Policy* (PO(2009)0141).

NATO. (2014, September). *NATO - Official text: Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO - EU Council. (2017a). *Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016*. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170619_170614-Joint-progress-report-EU-NATO-EN.pdf

NATO - EU Council. (2017b). *Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016*. https://www.consilium.europa.eu/media/35577/report-ue-nato-layout-en.pdf

NATO - EU Council. (2018). *Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*. https://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf

NATO - EU Council. (2019). *Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017*. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

NATO StratCom Centre of Excellence. (2018). *Hybrid Threats: Confucius Institute*. NATO StratCom Centre of Excellence. https://www.stratcomcoe.org/hybrid-threats-confucius-institutes

NATO StratCom CoE. (2019). *Hybrid Threats: A Strategic Communications Perspective*. NATO. https://www.stratcomcoe.org/download/file/fid/80212

NATO StratCom CoE. (2020a). *About Strategic Communications | StratCom*. https://www.stratcomcoe.org/about-strategic-communications

NATO StratCom CoE. (2020b). *About us | StratCom*. https://www.stratcomcoe.org/about-us

Nemr, C., & Gangware, W. (2019). *Weapons of mass distraction: Foreign State-sponsored disinformation in the digital age*. Park Advisors. https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf

Newnham, R. (2011, February). Oil, carrots, and sticks: Russia's energy resources as a foreign policy tool. *Journal of Eurasian Studies*, *2*, 134–143. https://www.academia.edu/16662374/Oil_carrots_and_sticks_Russia_s_energy_resources_as_a_foreign_policy_tool

newsinenglish.no staff. (2017, October). *Russians jammed flights' GPS* [News in English]. https://www.newsinenglish.no/2017/10/06/russians-jammed-flights-gps/

Nimmo, B., Barojan, D., & Aleksejeva, N. (2017). *Russian Narratives on NATO's Deployment*. DFRLab. https://medium.com/dfrlab/russian-narratives-on-natos-deployment-616e19c3d194

NIS Cooperation Group. (2020). *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* (No. 01/2020). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

Norberg, J. (2018). *Training for War—Russia's Strategic-level Military Exercises 2009-2017* (FOI-R--4627--SE; p. 110). Swedish Defence Research Agency - Ministry of Defence. https://www.foi.se/rest-api/report/FOI-R--4627--SE

Northstream. (2019). *5G Outlook in Europe*. http://northstream.se/northstreamwp/wp-content/uploads/2019/09/5G_Northstream_Opinion_.pdf

OECD. (2019). *Education at a glance 2019. OECD indicators*. https://doi.org/10.1787/f8d7880d-en

Office of the Director of National Intelligence. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* [Intelligence Community Assessment]. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Office of the United Nations High Commissioner for Human Rights. (2020). *Report on the human rights situation in Ukraine 16 November 2019 to 15 February 2020*. https://www.ohchr.org/Documents/Countries/UA/29thReportUkraine_EN.pdf

Oliveira, I. (2016, February). *National Front seeks Russian cash for election fight*. Politico.Eu. https://www.politico.eu/article/le-pen-russia-crimea-putin-money-bank-national-front-seeks-russian-cash-for-election-fight/

Open Society Institute Sofia. (2019, November). *The Media Literacy Index 2019: Just think about it*. Open Society Institute Sofia. https://osis.bg/?p=3356&lang=en

Ortega, A. (2020, February). *Digital decolonisation: The EU's new ideas on data and artificial intelligence*. European Council on Foreign Relations. https://www.ecfr.eu/article/commentary_digital_decolonisation_the_eus_new_ideas_on_data_and_artificial

OSCE. (2014). *Report of the Chief Monitor for the OSCE Special Monitoring Mission to Ukraine, Ambassador Ertugrul Apakan, to the OSCE Permanent Council*.

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Panda, A. (2018, February 20). *Three Years After Declaring Neutrality in Yemen Conflict, Pakistan to Send Troops to Saudi Arabia*. The Diplomat. https://thediplomat.com/2018/02/three-years-after-declaring-neutrality-in-yemen-conflict-pakistan-to-send-troops-to-saudi-arabia/

Panetta, K. (2017). *Gartner top strategic predictions for 2018 and beyond*. Gartner. https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/

Parker, N., Landay, J., & Walcott, J. (2017, April 19). *Putin-linked think tank drew up plan to sway 2016 US election—Documents*. Reuters. https://www.reuters.com/article/us-usa-russia-election-exclusive/putin-linked-think-tank-drew-up-plan-to-sway-2016-us-election-documents-idUSKBN17L2N3

Parliament of Australia. (2018). *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018*. https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6022

Peter, L. (2018, July). *Slovakia alarmed by pro-Putin Night Wolves bikers' base*. BBC News. https://www.bbc.com/news/world-europe-45019133

Peter, M., Alexander, S., Cambridge, A., Renee, S., Kang, R., Kiefer, S., Takayama, K., Laci, F., Michael, G., & Katie, M. (2019). *Combating targeted disinformation campaigns. A whole-of-society issue*. 2019 Public-private analytic exchange program. https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

Petraitis, D. (2019). The Anatomy of Zapad-2017: Certain Features of Russian Military Planning. *Lithuanian Annual Strategic Review - The Journal of Military Academy of Lithuania*, *16*. https://doi.org/10.2478/lasr-2018-0009

Petterson, R. (2017). *Outsourced to China. Confucius Institutes and Soft Power in American Higher Education*. National Association of Scholars. https://files.eric.ed.gov/fulltext/ED580866.pdf

Pew Research Center. (2017). *Europe's growing Muslim population*. https://www.pewforum.org/wp-content/uploads/sites/7/2017/11/FULL-REPORT-FOR-WEB-POSTING.pdf

Popescu, N. (2006). *Russia's Soft Power Ambitions* (Policy Brief No. 115). Centre for European Policy Studies. http://aei.pitt.edu/11715/1/1388.pdf

Portman, R., & Carper, T. (2019). *China's Impact on The U.S. Education System—Staff Report*. United States Senate - Permanent Subcommittee on Investigations - Committee on Homeland Security and Governmental Affairs. https://www.hsgac.senate.gov/imo/media/doc/PSI%20Report%20China's%20Impact%20on%20the%20US%20Education%20System.pdf

Qayyum, A., Qadir, J., Janjua, M. U., & Sher, F. (2019). Using Blockchain to rein in the new post-truth world and check the spread of fake news. *IT Professional*, *21*(4), 16–24. https://arxiv.org/pdf/1903.11899.pdf

Radford, A., Wu, J., Amodei, D., Clark, J., Brundage, M., & Sutskever, I. (2019, February 14). *Better language models and their implications*. OpenAI. https://openai.com/blog/better-language-models/

Radicalisation Awareness Network. (2019). *Preventing radicalisation to terrorism and violent extremism*. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-best-practices/docs/ran_collection-approaches_and_practices_en.pdf

Recknagel, C. (2014, March 28). *Complex Ties: Russia's Armed Forces Depend On Ukraine's Military Industry*. RadioFreeEurope. https://www.rferl.org/a/russia-ukraine-military-equipment/25312911.html

Rivera, R., Tarín, C., Villar, J. P., Ribagorda, A., Estévez, J. M., De Fuentes, J., & González, L. (2017). *Achieving a sovereign and trustworthy ICT industry in the EU*. European Parliament Research Service. http://www.europarl.europa.eu/RegData/etudes/STUD/2017/614531/EPRS_STU(2017)614531_EN.pdf

Robinson, N. (2019, August). *Australian universities risk catastrophe due to over-reliance on Chinese students, expert warns*. ABC News. https://www.abc.net.au/news/2019-08-21/australian-universities-too-dependent-on-chinese-students-report/11427272

Robinson, O., Coleman, A., & Sardarizadeh, S. (2019). *A report of anti-disinformation initiatives*. Oxford Technology & Elections Commission. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/08/A-Report-of-Anti-Disinformation-Initiatives

RTVE. (2018, January 25). *Stoltenberg sobre Cataluña: 'Es un asunto doméstico de España y la OTAN no debe involucrarse'—RTVE.es*. https://www.rtve.es/alacarta/videos/telediario/td2-otan-250118/4438218/

Rusnáková, S. (2017). Russian New Art of Hybrid Warfare in Ukraine. *Slovak Journal of Political Sciences*, *17*(3), 343–380. https://www.researchgate.net/publication/321955926_Russian_New_Art_of_Hybrid_Warfare_in_Ukraine

Sahlins, M. (2014, November 16). Confucius Institutes: Academic Malware. *The Asia-Pacific Journal. Japan Focus*, *12*. https://pdfs.semanticscholar.org/409b/c95e0f51e092652552c85e9f639b11c3fb5d.pdf?_ga=2.261689166.2125407473.1582539775-42699789.1579782498

Sanders, L. (2019, June). *Germany mulls requests to host Sea-Watch migrants*. Deutsche Welle (DW). https://www.dw.com/en/germany-mulls-requests-to-host-sea-watch-migrants/a-49243085

Sari, A. (2019). *Legal resilience in an era of grey zone conflicts and hybrid threats* (Working Paper No. 2019/1). Exeter Centre for International Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315682

Sari, A. (2020). *Hybrid threats and the law: Concepts, trends and implications*. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2020/04/Hybrid-CoE-Trend-Report-3.pdf

Sasse, G. (2017). *Revisiting the 2014 Annexation of Crimea*. Carnegie Europe - Carnegie Endowment for International Peace. https://carnegieeurope.eu/2017/03/15/revisiting-2014-annexation-of-crimea-pub-68423

Scheidt, M. (2019). *The European Union versus external disinformation campaigns in the midst of information warfare: Ready for the battle?* College of Europe. https://www.coleurope.eu/system/files_force/research-paper/edp_1_2019_scheidt.pdf?download=1

Schleicher, A. (2019). *PISA 2018—Insights and interpretations*. OECD. https://www.oecd.org/pisa/PISA%202018%20Insights%20and%20Interpretations%20FINAL%20PDF.pdf

Schreck, C. (2019). *From 'Not us' to 'Why hide it?': How Russia denied its Crimea invasion, then admitted it*. https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html

Schultz, T. (2017, February 23). *Why the 'fake rape' story against German NATO forces fell flat in Lithuania*. Deutsche Welle (DW). https://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870

Sciorilli, S. (2019, July). *Italian prosecutors investigate reports that League sought Russian funding*. Politico.Eu. https://www.politico.eu/article/italian-prosecutors-investigate-reports-that-league-sought-russian-funding-matteo-salvini-aide-gianluca-savoini/

Securities and Exchange Commission. (2015, November). *Securities and Exchange Commission v. James Alan Craig, (Civil Action No. 3:15-cv-05076)—Litigation Release No. 23401*. https://www.sec.gov/litigation/litreleases/2015/lr23401.htm

Segura, C. (2017, September). *Assange alienta que la rebelión en Cataluña se extienda a nivel global*. El País. https://elpais.com/ccaa/2017/09/26/catalunya/1506456387_836185.html

Selyukh, A. (2013, April 23). *Hackers send fake market-moving AP tweet on White House explosions*. Reuters. https://www.reuters.com/article/net-us-usa-whitehouse-ap/hackers-send-fake-market-moving-ap-tweet-on-white-house-explosions-idUSBRE93M12Y20130423

Shang, W., Liu, M., Lin, W., & Jia, M. (2018). *Tracing the source of news based on blockchain*. 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS),. https://ieeexplore.ieee.org/abstract/document/8466516

Shiraz, C. (2015, April 27). *Will Pakistan-Saudi relations survive Yemen crisis?* MO*. https://www.mo.be/en/analysis/will-pakistan-saudi-relations-survive-yemen-crisis

Siddiqui, N. (2019, December 21). *Saudi Arabia denies pressurising Pakistan to withdraw from Malaysia summit*. Dawn - World. https://www.dawn.com/news/1523518

Silvela, E. (2017). *La comunicación estratégica* (No. 72; Documentos de Seguridad y Defensa). Instituto Español de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/cuadernos/DocSeguridadyDefensa_72.pdf

Skinner, M. (2019, December). *The Financial Risk of Overreliance on Chinese Student Enrollment*. World Education News + Reviews. https://wenr.wes.org/2019/12/the-financial-risk-of-overreliance-on-chinese-student-enrollment

Smith, H. (2017). *In the era of hybrid threats: Power of the powerful or power of the "weak"?* Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2017/12/Strategic-Analysis-October-2017.pdf

Snegovaya, M. (2015). *Putin's information warfare in Ukraine. Soviet origins of Russia's hybrid warfare*. Institute for the Study of War. http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

Sommerbauer, J. (2016). *Die Ukraine im Krieg: Hinter den Frontlinien eines europäischen Konflikts* (Kremayr&Scheriau).

Spanish Government. (2019, February). *Referencia del Consejo de Ministros*. https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2019/refc20190215.aspx#CIBERSEGURIDAD

Spanish National Security Department. (2019). *National Cybersecurity Strategy 2019*. https://www.dsn.gob.es/en/documento/estrategia-nacional-ciberseguridad-2019

Starr, D. (2009). Chinese Language Education in Europe: The Confucius Institutes. *European Journal of Education*, *44*, 65–82. https://doi.org/10.1111/j.1465-3435.2008.01371.x

State Security Department of the Republic of Lithuania. (2019). *National Threat Assessment 2019*. State Security Department of the Republic of Lithuania - Ministry of National Defence. https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-EN.pdf

Stella, M., Ferrara, E., & De Domenico, M. (2018). Bots increase exposure to negative and inflammatory content in online social systems. *Proceedings of the National Academy of Sciences of the United States of America*. https://doi.org/10.1073/pnas.1803470115

Stern, D. (2017, June). *Lithuanians 'sleep peacefully' thanks to German troops*. Politico. https://www.politico.eu/article/lithuania-nato-russia-baltics-germany-sleep-peacefully-thanks-to-german-troops/

Stewart, S. (2009). Democracy promotion before and after the 'colour revolutions'. *Democratization*, *16*, 645–660. http://dx.doi.org/10.1080/13510340903082978

StopFake.org. (2020). *About us | Struggle against fake information about events in Ukraine*. https://www.stopfake.org/en/about-us/

Stratpol. (2016). *Panorama of global security environment 2015-2016*. https://stratpol.sk/wp-content/uploads/2016/05/panorama-2015-2016-FINAL.pdf

Sukhankin, S. (2017, September 8). Russia Tests EW Capabilities Ahead of Zapad 2017. *Eurasia Daily Monitor*, *14*. https://jamestown.org/program/russia-tests-ew-capabilities-ahead-of-zapad-2017/

Supreme Court Prosecutor. (2018). *Causa especial 3/20907/2017*. Supreme Court. https://cronicaglobal.elespanol.com/uploads/s1/39/18/31/0/392195369-conclusiones-provisionales-del-tribunal-supremo.pdf

Supreme Headquarters Allied Powers Europe. (2018). *NATO's Enhanced Forward Presence Battlegroup Lithuania Marks Its 4th Rotation*. SHAPE - Supreme Headquarters Allied Powers Europe. https://shape.nato.int/efp/latest-news/natos-enhanced-forward-presence-battlegroup-lithuania-marks-its-4th-rotation

Swedish Civil Contingencies Agency. (2018a). *Countering information influence activities—A handbook for communicators*. https://rib.msb.se/filer/pdf/28698.pdf

Swedish Civil Contingencies Agency. (2018b). *If crisis or war comes*. https://www.dinsakerhet.se/siteassets/dinsakerhet.se/broschyren-om-krisen-eller-kriget-kommer/om-krisen-eller-kriget-kommer---engelska-2.pdf

Sytas, A., Siebold, S., Martin, M., & Chopra, T. (2017, February 17). *Lithuania looking for source of false accusation of rape by German troops*. Reuters. https://www.reuters.com/article/us-lithuania-nato/lithuania-looking-for-source-of-false-accusation-of-rape-by-german-troops-idUSKBN15W1JO

Tajani, A. (2017, September). *Letter to Ms. Beatriz Basterrechea, MEP*. https://beatrizbecerra.eu/wp-content/uploads/2017/09/Respuesta-Tajani-Catalu%C3%B1a.pdf

Tasiu, A. (2018). Hostile gatekeeping: The strategy of engaging with journalists in extremism reporting. *Defence Strategic Communications - Officional Journal of the NATO Strategic Communications Centre of Excellence*, *5*, 51–85. https://www.stratcomcoe.org/download/file/fid/79989

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

The economist. (2017, August). *Putin the boots in Belarus—Russia's biggest war game in Europe since the cold war alarms NATO*. The Economist. https://www.economist.com/europe/2017/08/10/russias-biggest-war-game-in-europe-since-the-cold-war-alarms-nato

The Guardian. (2013, November 21). *Ukraine suspends talks on EU trade pact as Putin wins tug of war*. https://www.theguardian.com/world/2013/nov/21/ukraine-suspends-preparations-eu-trade-pact

The Lithuania Tribune. (2017, September). *Two Russian military aircraft violated Lithuanian airspace*. The Lithuania Tribune. https://lithuaniatribune.com/two-russian-military-aircraft-violated-lithuanian-airspace-foreign-ministry/

The White House. (1987). *National Security Strategy of the United States*. https://history.defense.gov/Portals/70/Documents/nss/nss1987.pdf?ver=2014-06-25-121104-753

The White House. (2010). *National Security Strategy*. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

The White House. (2017). *National Security Strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

The White House. (2020). *Executive order on preventing online censorship*. https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/

Tomkiw, L. (2018). *For Ukraine's wartime fact-checkers. The battle rages on*. Wilson Quarterly. https://www.wilsonquarterly.com/quarterly/the-disinformation-age/for-ukraines-wartime-fact-checkers-the-battle-rages-on/

Trembo, S. (2017, February 14). *Seimas ratified Defence Cooperation Agreement with the USA*. Lietuvos Respublikos Seimas. https://www.lrs.lt/sip/portal.show?p_r=119&p_k=2&p_t=169440

Treverton, G., Thvedt, A., Chen, A., Lee, K., & McCue, M. (2018). *Addressing Hybrid Threats*. Hybrid COE. https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf

UK Government. (2011). *Prevent strategy* (Cm 8092). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

UK Government. (2017). *The government response to the eight report from the Home Affairs Select Committee session 2016-17, HC 135: Radicalisation : the counter-narrative and identifying the tipping point* (Cm 9555). https://www.parliament.uk/documents/commons-committees/home-affairs/Correspondence-17-19/Radicalisation-the-counter-narrative-and-identifying-the-tipping-point-government-response-Eighth-Report-26-17-Cm-9555.pdf

UK Government. (2020, January 28). *Foreign Secretary's statement on Huawei*. https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei

UK Ministry of Defence. (2019). *Defence Strategic Communication: An approach to formulating and executing strategy* (Joint Doctrine Note No. 2/19). Development, Concepts and Doctrine Centre. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804319/20190523-dcdc_doctrine_uk_Defence_Stratrategic_Communication_jdn_2_19.pdf

United Nations Security Council. (2014). *REVIVAL OF ISLAMIC HERITAGE SOCIETY*. United Nations Security Council. https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/revival-of-islamic-heritage-society

University Foreign Interference Taskforce. (2019). *Guidelines to counter foreign influence in the Australian university sector*. https://docs.education.gov.au/system/files/doc/other/ed19-0222_-_int_-_ufit_guidelines_acc.pdf

US Department of Defence. (2008). *Principles of Strategic Communication*. https://www.hsdl.org/?view&did=716398

US Senate. (2019). *Report of the selected committee on intelligence on Russian active measures campaigns and interference in the 2016 U.S. election. Volume 1: Russian efforts against election infrastructure with additional views*. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

Vendil, C., & Oxenstierna, S. (2017). *Russian Think Tanks and Soft Power* (FOI-R-4451-SE). FOI - Swedish Defence Research Agency. https://www.foi.se/rest-api/report/FOI-R--4451--SE

Vidalon, D. (2019, November). *France will not exclude China's Huawei from 5G rollout: Minister*. Reuters. https://www.reuters.com/article/us-france-huawei-minister/france-will-not-exclude-chinas-huawei-from-5g-rollout-minister-idUSKBN1XZ1U9

Vikmanis, V. (2017, October 28). *Electronic War—Are We Ready? Zapad-2017 training*. Latvijas Avīze. https://www.la.lv/elektroniskais-kars-vai-esam-gatavi

Vojtíškova, V., Novotný, V., Schmid-Schmidsfelden, H., & Potapova, K. (2016). *The Bear in Sheep's Clothing—Russia's Government-Funded Organisations in the EU*. Wilfried Martens Centre for European Studies. https://www.martenscentre.eu/sites/default/files/publication-files/russia-gongos_0.pdf

von der Leyen, U. (2019). *A Union that strives for more. My agenda for Europe*. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

Vrije Universiteit Brussel. (2019, December). *The VUB will not continue its cooperation with the Confucius Institute*. https://press.vub.ac.be/the-vub-will-not-continue-its-cooperation-with-the-confucius-institute#

Warrell, H. (2019). *Britain to review Prevent anti-radicalisation programme | Financial Times*. https://www.ft.com/content/b4cc0fde-1e5f-11e9-b2f7-97e4dbd3580d

Warsaw Institute. (2017). *ZAPAD - 2017. Lessons Learned*. The Warsaw Institute Foundation. https://warsawinstitute.org/wp-content/uploads/2017/10/ZAPAD-2017-russia-belarus-military-manuovers-drills-summary-eng.pdf

Wilson, A. (2014). *Ukraine Crisis: What it means for the West*. Yale University Press.

Wilson, P., & Kennedy, A. (1999). Trustworthiness as an Economic Asset. *International Food and Agribusiness Management Review*, *2*(2), 179–193. https://www.ifama.org/resources/Documents/v2i2/Wilson-Kennedy.pdf

Yousaf, F. (2016). *The plight of Religious Minorities in Pakistan*. South Asia Democratic Forum. https://www.researchgate.net/publication/324245465_SADF_Focus_The_plight_of_Religious_Minorities_in_Pakistan

Zhukov, Y. (2015). *The economics of rebellion in Eastern Ukraine*. Vox Ukraine. https://voxukraine.org/en/the-economics-of-rebellion-in-eastern-ukraine/

ANNEXES

Methodology and resources used

Two main methodological resources have been used to perform the analysis of hybrid threats and strategic communications. The first one has been a detailed desk research, taking into account an extensive collection of documents that can be consulted in the References section.

The second resource has been interviews with key experts in the topic. The following experts were interviewed during the project. We want to thank them for their valuable ideas and contributions:

- Georgios Chatzichristos, Member of the Operational Security Unit at ENISA.
- CN Enrique Cubeiro, Chief of Staff at the Spanish Joint Cyber-Defence Command.
- Gustav Gressel, Senior Policy Fellow within the Wider Europe Programme at the European Council on Foreign Relations.
- Lutz Guellner, Head of Division of Strategic Communications at the European External Action Service.
- Irene Lozano, former Secretary of State of España Global. Spanish Government.
- Jānis Sārts, Director of the NATO Strategic Communications Centre of Excellence.
- Elvira Tejada de la Fuente, Chief Prosecutor of the Computer Criminal Unit. State Attorney General of Spain.
- Dr. Teija Tiillikainen, Director of the Hybrid CoE, the European Centre of Excellence for Countering Hybrid Threats.
- Veronika Víchová, Head of the Kremlin Watch Program at the European Values Think-tank.

OA-02-21-202-EN-N

This study describes the key features, technologies and processes involved in strategic communications to counter hybrid threats and their components.

A theoretical description of hybrid threats is complemented by an analysis of diverse case studies, describing the geopolitical context in which the hybrid threat took place, its main features, the mechanisms related to strategic communications used by the victim to counter the hybrid threat and its impact and consequences.

This is a publication of the Scientific Foresight Unit (STOA)
EPRS | European Parliamentary Research Service

ISBN 978-92-846-7812-9 | doi: 10.2861/14410 | QA-02-21-202-EN-N