

Master in Advanced European and International Studies

Applied European Policy and Governance Studies

*Navigating Hybrid Threats: Is
NATO–EU Cooperation a Catalyst
or Constraint in Combatting
COVID-19 Disinformation?*

Supervised by George Tzogopoulos

Fuzè Sentenach Berástegui

2025



Co-funded by
the European Union

Acknowledgements

I would first like to express my deep appreciation to the Centre International de Formation Européenne (CIFE) for providing an intellectually stimulating and multicultural environment throughout this academic year. The programme has been a truly transformative experience, and I am grateful for the opportunities to grow, learn, and exchange ideas while working on this thesis.

My special thanks go to my thesis supervisor, George Tzogopoulos, for his thoughtful guidance and consistent support during the research and writing process. I would also like to thank the programme director, Susann Heinecke-Kuhn, and my professors, especially Anna Dimitrova, who took the time to offer feedback and direction. Their expertise and encouragement helped shape the final result.

Lastly, I am especially grateful to my family and friends, whose encouragement, patience, and belief in me have been invaluable. Their support carried me through moments of doubt and motivated me to keep pushing forward.

Abstract

This thesis questions the disinformation development of the North Atlantic Treaty Organisation (NATO) and the European Union (EU) as a strategic element in hybrid threats and evaluates their interventions to face it, especially during the COVID-19 pandemic. Tracing through Hybrid Threat Theory (HTT) and Resource Dependence Theory (RDT), the study evaluates how both organisations have responded and whether their cooperation added value in countering disinformation.

An empirical qualitative case-study methodology is used and it combines both primary institutional documents and secondary academic literature. The analysis outlines NATO's military-oriented strategic communication drawn up in comparison to the EU's normative-regulatory mechanisms such as the Digital Services Act (DSA) and the Code of Practice on Disinformation that the EU has developed to outline their strengths and limitations. The COVID-19 pandemic case-study serves as a stress test concerning whether the two institutions are capable of working together in order to effectively counter hybrid threats.

These outcomes indicate that, although their strategies are complementary, coordination is threatened by institutional stovepipes, mandate asymmetries, and divergent strategic cultures. New initiatives such as the Hybrid Centre of Excellence (Hybrid CoE) and the Joint Declarations on EU-NATO cooperation, however, bring an incremental progress toward more integrated hybrid threat governance. This thesis contributes to existing high-pressure context of hybrid security and transatlantic governance by evaluating their institutional interplay. It claims that a cohesive and anticipatory strategy is essential to safeguarding democratic resilience in an increasingly contested digital environment.

Table of contents

List of abbreviations	4
Introduction	5
Chapter 1. Understanding Hybrid Threats and Disinformation	9
1.1 The Evolution of Hybrid Threats: from Traditional Warfare to Strategic Ambiguity.....	10
1.2 Disinformation as a Hybrid Threat	14
1.3 NATO & the EU: why Hybrid Threats and Disinformation are now a strategic priority	16
Chapter 2. NATO’s approach to Hybrid Threats	19
2.1 NATO responses to Hybrid Threats	21
2.2 NATO’s recognition of Disinformation as a Hybrid Threat.....	23
2.3 Institutional constraints and internal divergence in NATO’s response	27
Chapter 3. EU’s strategic response to Hybrid Threats	31
3.1 The EU’s frameworks against Disinformation	33
3.2 Strategic communication and resilience tools.....	36
3.3 Gaps, challenges and opportunities in the EU’s Disinformation strategy	38
Chapter 4. Case study: NATO-EU cooperation during the COVID-19 pandemic	44
4.1 Strategic use of Disinformation during the COVID-19 pandemic	46
4.1.1 Weaponizing the crisis: exploiting fear and uncertainty	46
4.1.2 State-sponsored propaganda and conspiracy theories.....	47
4.1.3 Technical amplifiers: social media, bots and AI.....	49
4.1.4 Institutional vulnerabilities: crisis communication and trust deficits.....	50
4.2 NATO-EU responses: diverging logics, complementary strategies.....	51
4.2.1 NATO’s strategic response to COVID-19 Disinformation	52
4.2.2 The EU’s regulatory and normative approach.....	53
4.3 Evaluation of joint response: strengths, weaknesses, and lessons learned.....	56
Conclusions and critical reflection	63
Bibliography	66

List of abbreviations

AI – Artificial Intelligence

COVID-19 – Coronavirus Disease 2019

DSA – Digital Services Act

EEAS – European External Action Service

EDAP - European Democracy Action Plan

EDMO – European Digital Media Observatory

EU – European Union

EUvsDisinfo – European Union vs Disinformation

FIMI – Foreign Information Manipulation and Interference

G7 – 7 major industrial countries formed by Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, and the European Union

HTT – Hybrid Threat Theory

Hybrid CoE – European Centre of Excellence for Countering Hybrid Threats

NATO – North Atlantic Treaty Organization

OSCE – Organisation for Security and Cooperation in Europe

RDT – Resource Dependence Theory

RT – Russia Today (Russian state-controlled media outlet)

StratCom – Strategic Communications

StratCom COE – Strategic Communications Centre of Excellence (NATO)

UN – United Nations

VLOPs – Very Large Online Platforms

Introduction

“Disinformation is not merely a problem of false information, but a strategic weapon designed to manipulate perceptions, erode trust, and destabilize democratic institutions” (Pamment, 2020)

In the current discussion of modern security, the statement of Pamment captures the growing recognition that challenges are no longer defined solely by tanks and missiles, but increasingly by cognitive and informational vulnerabilities. The 21st century global security environment has therefore experienced a fundamental transformation as traditional notions of warfare, centred on open, state-versus-state conflict, have been steadily replaced by more complex, ambiguous, and multifaceted forms of threat. One of the most notable examples of this developing paradigm is the rise of hybrid threats: a term that covers the blending of conventional military force with non-traditional instruments of coercion such as cyberattacks, economic pressure, disinformation, and political subversion. These threats operate in the so-called “grey zone,” deliberately remaining below the threshold of open armed conflict in order to avoid conventional deterrence and complicate attribution and response (Giegerich, 2016; Hoffman, 2010).

Hybrid threats challenge the foundations of national and international security by targeting not only physical infrastructure but also the cognitive and informational landscapes of societies. Among the most significant components of hybrid warfare is disinformation, the deliberate dissemination of false, misleading, or manipulated information with the intent to deceive, destabilize, or influence public opinion and institutional legitimacy (Pamment, 2020). Unlike conventional military threats, disinformation operates through information networks and often relies on social media platforms and digital technologies to amplify false narratives, polarize societies, and erode democratic resilience. As a result, disinformation has become not merely a communication problem but a strategic weapon within the broader hybrid threats.

The COVID-19 pandemic offered a high-impact, real-life demonstration of disinformation’s potential as a security threat. As governments struggled to respond to an unprecedented public health crisis, malicious states and non-state actors exploited the atmosphere of fear, uncertainty, and institutional stress to launch coordinated disinformation campaigns. These efforts not only aimed to threaten public confidence in vaccines and government responses, but also to challenge the credibility of transatlantic institutions such as the European Union (EU) and the North

Atlantic Treaty Organization (NATO) (Tagliabue, Galassi, & Mariani, 2020; Chłoń, 2022). The pandemic thus offers a particularly revealing case study for analysing institutional responses to disinformation under conditions of systemic stress and hybrid threat escalation.

Given the growing rate of disinformation campaigns in Europe, the premise of this thesis is the following research question: How has NATO addressed the challenge of disinformation in Europe, and how has its complementary collaboration with the EU enhanced efforts to counter disinformation during the COVID-19 pandemic? To answer this, the study adopts a comparative and cooperative framework which analyses both institutions' distinct approaches and their joint response mechanisms. That question is not only timely but necessary, as it explains how Europe's core security and governance actors are adapting to an evolving hybrid threat scenario.

This research is guided by four interrelated objectives. First, a conceptual foundation is developed by framing hybrid threats and disinformation as complex and evolving security challenge. Second, it traces the conceptual and strategic evolution in NATO's approach to disinformation and positions it within the broader hybrid threat doctrine and strategic communications. Third, it investigates the EU's regulatory and normative framework, that is the Digital Services Act (DSA), the Code of Practice on Disinformation, and the European Democracy Action Plan (EDAP), to evaluate their proposed goals and operationalisation. Fourth, it assesses critically the effectiveness of EU-NATO cooperation throughout the pandemic, pointing out their institutional strengths, weaknesses as well as the lessons learnt.

The thesis examines the period between 2019 to 2022, encompassing the most uncertain phases of the pandemic and the associated disinformation campaigns. This timeframe also aligns with major strategic developments in both institutions including NATO's updated Strategic Concept and the EU's implementation of the new legislative and policy frameworks. Geographically, the focus is on the Member States of NATO and the EU, with the emphasis placed on Eastern Europe and the Baltic region, the areas which are especially vulnerable to disinformation due to their proximity to Russia and the historical exposure to influence operations (Arcos & Smith, 2021).

The theoretical foundation of this thesis is founded on two theoretical lenses. Hybrid Threat Theory (HTT) provides a strategic framework through which to analyse how disinformation interacts with cyberattacks, economic pressure, and political interference targeting democratic

systems (Hoffman, 2010; Hartmann, 2017). In parallel, Resource Dependence Theory (RDT) explains how institutional collaboration arises as the result of complementary needs and capabilities: NATO has military and crisis management resources, while the EU offers regulatory and normative tools (Anagnostakis, 2025; Van Raemdonck & Meyer, 2024). The combination of these analytical frameworks helps demonstrate that there are reasons to inter-institutional cooperation, as well as structural barriers that further complicate it.

Methodologically, the research uses a qualitative research design that has been formed by document analysis. It is based on a wide range of primary sources, such as NATO summit declarations, strategic doctrines, and public communications, alongside EU legislative texts, policy communications, and institutional reports. Particular attention is given to institutional actors such as NATO's Strategic Communications Centre of Excellence (StratCom COE), the EU's East StratCom Task Force, and the European Digital Media Observatory (EDMO). Secondary sources from academic publications, policy think tanks, and independent monitoring organisations are added to provide contextual analysis and interpretive depth. This approach allows for a critical comparison of NATO's and the EU's narratives and strategies in countering hybrid threats and disinformation.

Empirically, the core of this thesis is a case study of disinformation in the COVID-19 pandemic. Chosen due to its contemporary relevance and its ability to show hybrid threats using operational crisis to reach strategic goals, this example shows how coordinated influence operations attacked both NATO and the EU in their attempt to erode public trust, irrecoverably paralyse crisis response, and create uncertainty regarding the origin of the virus as well as its management. These campaigns were characterised by the extensive use of digital platforms, automated bots, manipulated imagery, and conspiracy theories to develop and spread false narratives (Ferreira Caceres et al., 2022). In response, NATO reacted issuing public rebuttals, launching strategic communication initiatives, and strengthening internal coordination. At the same time, the EU acted to enforce regulatory measures to increase platform accountability and supported civil society actors engaged in fact-checking and promote digital literacy (European Commission, 2022; Genini, 2025).

The aim of this thesis is not only to assess how NATO and the EU have individually responded to the challenge of disinformation but also to critically evaluate whether their inter-institutional

cooperation has created effective added value when dealing with the rapidly evolving and changing hybrid threats. In doing so, it will provide an insight into the ongoing adaptation of Europe's core security and governance institutions, highlighting the pathways and possible challenges to developing a stronger democratic resilience in an increasingly complex and contested information environment.

Chapter 1. Understanding Hybrid Threats and Disinformation

In the 21st century, global security has been under significant transformations, with hybrid threats becoming one of the most complex and pervasive challenges that both states and international organisations face. Unlike traditional security, which were mostly military in nature up until recently, hybrid threats involve a complex set of coercive measures that combine conventional military force with unconventional tactics such as cyber warfare, economic pressure, and disinformation. Furthermore, such threats operate on the ambiguous spaces between war and peace where attribution is difficult, responses are complicated, and the effects are often cumulative and strategically significant (Giegerich, 2016).

Disinformation, in particular, has emerged as a core component of hybrid warfare strategies, as “it is aimed at manipulating public opinion, eroding trust in democratic institutions, and destabilizing political environments without requiring any direct kinetic engagement” (Pamment, 2020). Rapid dissemination of information has grown with the proliferation of digital platforms and the consequent wide spreading of information which has increased the impact and extend to which disinformation reaches. Social media ecosystems, new platforms, and emerging technologies are utilised by both state and non-state actors to shape narratives, spread falsehoods, and provoke societal divisions (Filipec, 2021). As a result, organizations like the North Atlantic Treaty Organisation (NATO) and the European Union (EU) have had to adjust their strategic thinking and accordingly view disinformation, not only a communications issue, but as a direct security threat to democratic governance, societal cohesion, and transatlantic security (Treverton et al., 2023).

The current chapter lays down the conceptual foundation of the thesis and describes hybrid threats and disinformation as an evolving and multidimensional security challenge. It begins by providing an overview of hybrid warfare, tracing its evolution from traditional military conflict to today’s ambiguous, multi-domain forms of strategic competition. It subsequently examines the development of disinformation as a key instrument within hybrid operations, not only as a tool of deception but as a cognitive and societal weapon that targets the foundations of democratic systems. Lastly, the chapter analyses how NATO and the EU have integrated hybrid threat and strategic disinformation in their strategic agendas, drawing on Hybrid Threat Theory (HTT) and Resource Dependence Theory (RDT) to explain the institutional dynamics, vulnerabilities, and interdependencies that shape their responses.

By combining these theoretical frameworks, the chapter can establish the theoretical and analytical framework upon which the rest of the thesis builds, informing the subsequent analysis of NATO's evolving posture (Chapter 2), the EU's regulatory and resilience-building strategies (Chapter 3), and the coordinated response of both organisations during the COVID-19 pandemic (Chapter 4).

1.1 The Evolution of Hybrid Threats: from Traditional Warfare to Strategic Ambiguity

The nature of global security has experienced radical changes throughout the past few decades. Traditional security threats, which traditionally were characterized by state-on-state warfare, conventional military engagements and clearly defined frontlines, have gradually transformed into a more complex and multifaceted security landscape. The rise of hybrid threats represents “a significant shift into how conflicts are conducted, blurring the lines between war and peace, state and non-state actors, and military and civil domains” (Hartmann, 2017).

Historically, security threats were defined within the framework of conventional warfare. States relied on military strength, deterrence through force, and formal declarations of war to attain their goals. The Cold War was indeed the pattern of the security relations, which was the bipolar struggle between NATO and Warsaw Pact, where the major concentration largely rested on nuclear deterrence and large-scale conventional military engagements (Hartmann, 2017). However, in the post-Cold War era, this tendency took a valuable shift towards asymmetric conflicts, irregular warfare, and new forms of non-traditional security challenges. Globalisation, technological advancements and the increasing role of non-state actors in the security discourse were some factors that triggered these changes.

The recent change in global threats has led to the recent transformation and evolution of hybrid threats. Unlike traditional conflicts where the military provided all the tools necessary to engage in conflict, hybrid threats incorporate a full range of different modes of warfare such as conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. They can be defined as any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behaviour in the battlespace to obtain their political objectives (Hoffman, 2010). These threats are based on societal vulnerabilities, target critical infrastructure, and

undermine democratic institutions without necessarily triggering a formal military response (Balogh, 2020).

A critical framework of examining this phenomenon is developed by Pawlak (2015, 2017). He defines hybrid threats as ambiguous and gradual, strategically leveraging the grey zone between war and peace, where adversaries pursue strategic goals through a combination of military, non-military, and unconventional tactics. This framework also highlights the complexity of hybrid threats, showing how they exploit both state and societal vulnerabilities to create an environment of strategic uncertainty (Pawlak, 2015).

This implementation of the grey zone concept mirrors the challenges discussed by Giegerich (2016) and Freedman (2017), according to whom hybrid threats are specifically designed to avoid straightforward military solutions. Operationally, according to Giegerich (2016), "hybrid threats are designed to be ambiguous, fast-moving, and deniable, often combining the use of proxies, strategic communication campaigns, cyber intrusions, and economic pressure to destabilize adversaries". As hybrid threats present a serious challenge to the foundational assumptions of conventional deterrence and defence strategies, organisations like NATO and the EU are forced to develop a more agile and comprehensive approach to security. Freedman (2017), in his monograph "The Future of War: A history", points out that the future of conflict lies less in open battlefields and more in the manipulation of political, social and informational environments. He notes that the modern adversaries are increasingly adept at shaping perceptions, narratives, and public opinion, which makes information dominance one of the most critical elements of strategic competition.

As a result, hybrid threats can be considered both military and broader societal and political phenomena. Their multidimensional nature makes them particularly challenging to counter since they operate within the "grey zone" of conflict, which is below the threshold of open warfare but having significant strategic consequences (Hoffmann, 2010). Plausible deniability, incremental aggression, and the use of multiple instruments of power simultaneously, such as economic pressure, cyberattacks, disinformation, political subversion, and limited conventional force are contextualisation of the grey zone. Actors like Russia during the annexation of Crimea or China in the South China Sea, represent such an approach, deliberately opting out of escalation in favour of a steadily achievement in strategic gains (Giegerich, 2016). This ambiguity

of tactics creates harsh dilemmas on the decision-making of traditional security organisations: how to attribute attacks, assess proportional responses, and maintain unity among allies. As Freedman (2017) accurately notes, “deterrence becomes further complicated as adversaries seek gradualism and ambiguity over clear, decisive actions by requiring defence planners to adjust the current structures accordingly”.

Successfully operating in the grey zone requires resilience, strategic communication superiority, intelligence cooperation, and a readiness to respond across multiple domains simultaneously. Krulak (1999) recognises the capacity of low-ranking actors, specifically when enhanced by digital media and social networks, to cause strategic consequences that eventually eclipse their initial positions well after the fight. When disinformation is applied to a single event, whether by manipulating or misinterpreting the occurrence, it has the potential to cause political crises, undermine legitimacy, or escalate tensions in unforeseen ways due to the increasing reliance on digital technology, social media, and interconnected global markets. Over the last several years, interested actors, both state and non-state, have increasingly used these tools to pursue strategic objectives without engaging in direct military confrontation. The result of this has been that disinformation campaigns, cyberattacks, and election interference have become prominent elements of hybrid warfare as it has been used to target public trust in democratic institutions and to create social and political instability (Ivancik, 2023). Since these hybrid threats keep evolving, it is important to understand that they present systemic challenges to military alliances like NATO, as well as the security and stability of democratic societies as whole. These abilities of hybrid actors to exploit existing societal fractures, such as political polarization, economic instability, and information vulnerabilities, highlights the need for a comprehensive and adaptive security strategy (Hoffmann, 2010). In turn, leadership at all levels should now be ready to navigate in complex, multi-domain environments, where tactical actions, now amplified through digital media, can have immediate and disproportionate strategic outcomes (Krulak, 1999).

Nowadays, hybrid threats are a flagship of global security. They have now gone beyond the jurisdiction of state actors as terrorist organizations, criminal networks, and even private entities are increasingly adopting hybrid tactics in order to achieve their goals. The development of artificial intelligence, deepfake technology, and sophisticated cyber tools has even further expanded the range and effectiveness of hybrid threats, making them more difficult to detect and counter (European Commission, 2020). These changes require a shift towards an adaptive

and comprehensive security strategies that combines military, civilian and technological capacities.

Understanding these evolving threats through both Hybrid Threat Theory (HTT) and Resource Dependence Theory (RDT) enables a critical evaluation of institutional adaptation and cooperation, particularly in cases like the COVID-19 pandemic, where strategic ambiguity intersected with public health vulnerability. To conceptualise the complexity on hybrid threats and institutional responses, this thesis combines these two conceptual theories.

On the one hand, Hybrid Threat Theory (HTT) states the integrated use of military and non-military instruments, including cyberattacks, disinformation, and political interference, with the aim to infiltrate the cognitive and societal system of democratic states below the threshold of conventional warfare (Hoffman, 2010; Hartmann, 2017). HTT provides a theoretical foundation to tracking the evolution of disinformation as a peripheral concern onto the core strategic threat that requires multidimensional countermeasures. Resource Dependence Theory (RDT), on the other hand, provides an organisational lens to explain the dynamics of inter-institutional cooperation in responding to hybrid threats. RDT insists that organisations establish partnerships to mitigate internal resource constraints, be these technical capabilities, regulatory mandates, legitimacy, or outreach tools (Anagnostakis, 2025). In such an analytical framework, NATO, with its military and deterrence expertise but limited civilian regulatory authority, and the EU, with normative and regulatory competencies but lacking strong external security mandate, makes a complementary strategic partnership. Therefore, their collaboration on disinformation is based on mutual dependencies, as NATO relies on the EU's civilian tools, and the EU benefits from NATO's intelligence and security systems (Milo, 2021; Filipec, 2021).

Together, HTT and RDT offer both analytical lens through which to explore the responses of NATO and the EU to disinformation as a hybrid threat individually and collectively. Chapters 2, 3 and 4 follow on this by looking at the strategic adaptation of NATO (Chapter 2), the regulatory and resilience-building approaches of the EU (Chapter 3), and the coordinated by both organisations to response to the COVID-19 pandemic (Chapter 4). These analyses go further than describing the policy but rather explore how institutional boundaries are being defined and how these hybrid threats are fostering developing interdependence within the transatlantic security landscape.

1.2 Disinformation as a Hybrid Threat

Hybrid threats have evolved to target not only attack military assets but are now also directed against the societal foundations on which states exist, and disinformation is now a critical and powerful tool of influence and destabilisation. Its role to hybrid warfare goes beyond misleading, but strategically weakens, disorients, destabilizes, disrupts political structures and fragments societies undermining political structures, state functionality, and public trust. Due to the fact that such operations often occur without triggering formal conflict, disinformation is especially successful in the ambiguous terrain of hybrid threats.

In theory, disinformation is closely connected to the notions of false news and propaganda, terms which are quite often confused or used as synonyms in the public debate (Ivančík & Nečas, 2022). However, key distinctions exist. Some authors consider false reports to be all reports that are not underpinned by facts but instead published as such (Allcott & Gentzkow, 2017) or any report that deny the principles of quality and objective journalism (Baym, 2005). Others, in their turn, distinguish between media which spread false news and the so-called political media that regulates news to set the political agenda of a certain political party or movement (Vargo et al., 2017).

Despite the increased visibility of disinformation in the current security threat landscape, its strategic use is far from new, it is not an achievement of the 21st century or today's information society. As early as the 6th century BC, Chinese general Sun Tzu wrote in his "Art of War" about the doctrine of indirect combat by using lies and false, fraudulent reports. Textbook examples of the use of disinformation in practice can also be found in ancient Greece from the Greco-Persian wars (Ivančík & Nečas, 2022). What has changed in the first two decades of the third millennium is the scale, speed and sophistication, enabled by digital technologies, mass connectivity and social media.

The modern information ecosystem is defined by the ability to provide tailored content delivery, algorithmic amplification, and microtargeting, which altogether allow false narratives to reach and influence segmented audiences with unprecedented efficiency. As a result, disinformation ceased being a blunt tool of deception and became a weaponised narrative strategy, used to manufacture legitimacy, widen social fragmentation, and shape political realities. Social media,

plays a crucial role within this context providing low-cost, high-impact channels through which hybrid actors attempt to control and manipulate public discourse and perception.

From a hybrid threat perspective, the spread of disinformation is a major security threat since it undermines citizens' trust in democratic institutions, delegitimises political processes and intensifies societal polarisation. Studies prove that disinformation campaigns are often based on conservative political agendas, exploiting fears about migration, multiculturalism, or state authority (Prier, 2017). These narratives are often propagated through websites that mimic legitimate news sources but are used to achieve an ideological or commercial purpose. On the pretence of presenting credible journalism, such sites erode the credibility of traditional media and blur the boundary between factual facts and manipulation tactics. One of the key drivers of this phenomenon is the structure design of social media, which gives rise to the development of echo chambers or homophilic networks, where users are mostly exposed to like-minded views. Such an arrangement also strengthens cognitive biases, most notably confirmation bias and limits openness to dissenting perspectives. In these self-contained digital environments, disinformation not only becomes much easier to internalise but harder to correct later. As Prier (2017) notes, "once people believe misinformation as truth within such bubbles, it may lead to radicalisation and the weakening of societal cohesion".

In the current digital age, disinformation has become not only a distortion of facts but also a strategic weapon that hybrid threat actors can use to weaken adversaries cognitively and politically. In the perspective of HTT, it is a non-military instrument that harmonises with cyberattacks and economic coercion, and its aim is to weaken democratic stability (Hoffman, 2010). Launched alongside cyberattacks, economic pressure and legal subversion, disinformation is a critical axis of hybrid warfare. Moreover, from the lens of RDT, disinformation reveals critical institutional gaps that make cooperation necessary. Neither NATO, which wields military expertise and limited regulatory authority, nor the EU, which has normative and civilian tools but limited coercive capacity, can neutralise the complex threat of disinformation on their own. Their collaborative approach is therefore an adaptive response to mutual dependencies, where each organisation supplies capabilities that the other lacks (Anagnostakis, 2025).

To sum up, disinformation is a strategy that is used both as a form of hybrid warfare and as a means to influence the cognitive environment undermining institutional legitimacy,

manipulating societal beliefs, and polarising political discourse. Its core function in contemporary hybrid operations highlights the need for coordinated multidimensional countermeasures. So, in order to safeguard democratic societies against this new and increasing threat, military and civilian institutions must move beyond the artificial strategies and embrace common frameworks that foster digital literacy and enhance societal resilience.

1.3 NATO & the EU: why Hybrid Threats and Disinformation are now a strategic priority

The concept of hybrid threats has become central to the state-level strategies and initiatives of international organisations. It has summarised the increasing complexity of contemporary security challenges, where adversaries combine conventional and unconventional tools - military, cyber, economic, informational - to reach strategic objectives below the threshold of armed conflict. In turn, the European Union (EU) and the North Atlantic Treaty Organisation (NATO) have explicitly recognised hybrid threats as a pressing challenge, integrating them into their respective doctrines, planning frameworks, and capacity-building efforts (Arcos & Smith, 2021). This awareness is consistent with HTT, where integrated use of both military and non-military tools based on exploiting vulnerabilities below the threshold of conventional warfare is emphasised (Hoffman, 2010).

The EU defines hybrid threats as “the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological) that can be employed by state or non-state actors in a combined manner to reach specific objectives while remaining below the threshold of formally declared warfare” (European Commission, 2016: 2). NATO, for its part, categorises hybrid threats as “the coordinated use of military and non-military tactics designed to destabilize societies without triggering collective defence mechanisms” (NATO, 2024). These definitions reflect a shared understanding that hybrid threats aim to create confusion, delay political decision-making, and undermine social cohesion, often through the weaponisation of information and the erosion of trust towards democratic institutions.

One of the most widely known manifestation of hybrid threats is disinformation. Unlike traditional forms of propaganda, contemporary disinformation campaigns are enhanced with the digital technologies and are designed to disrupt societies internally by targeting cognitive vulnerabilities. Such operations do not only aim at misleading but to polarising, fragmenting, and delegitimising democratic processes. Although propaganda and psychological operations are

longstanding tactics of statecraft, today's digital ecosystem, particularly social media, has increased their reach, speed, and sophistication. HTT explains how these operations weaponise the cognitive domain by manipulating the narrative and framing the perceptions on both societal and individual levels.

Within NATO and the EU alike, disinformation has been transformed from a marginal concern to a core strategic priority, particularly after its sudden rise during the COVID-19 pandemic. Hostile actors, both state and non-state, capitalised on the crisis to call into question the credibility of public health measures, propagate anti-Western narratives, and cause discord among allies. This episode demonstrated the permeability of the information domain and reinforced the idea that hybrid threats transcend the traditional distinctions between internal and external security.

An early recognition of the strategic implications of hybrid interference can be traced back to the 2015 Food-for-Thought Paper by the European External Action Service (EEAS), recommending the establishment of a cross-sectoral coordination, joint situational awareness, and improve institutional preparedness. This informal paper formed the basis on which further policy making was formulated, including the 2016 Joint Communication on Countering Hybrid Threats and the creation of the East StratCom Task Force (EEAS, 2015). Such initiatives were the turning point in the establishment of institutional awareness, especially on the need to engage in multi-level, multi-domain cooperation.

Resource Dependence Theory (RDT) supports the cooperative imperative observed in the current international security environment and explains why and how institutions pursue cooperative partnerships to address gaps in their capabilities. No individual state or organisation, military or civilian, has all the resources needed to confront hybrid threats on its own. NATO and the EU are an example of this principle: NATO's intelligence, operational coordination, and strategic communication capabilities complements the EU's legal, regulatory, and civil society tools. As Biermann and Harsch (2021) points out, inter-organisational collaboration often emerges out of asymmetric dependencies, in which each of the actors bring different resources to offer while seeking legitimacy and effectiveness.

In addition, convergence of security domains, including military, informational, technological, and legal, requires institutions to develop responses that are convergent and adaptable. Such

hybrid threats are frequently transboundary and transnational, requiring not merely intelligence sharing or coordinated messaging but also institutional resilience. As a countermeasure, NATO and the EU have reacted to this by adapting and integrating hybrid threat preparedness into planning processes and by enhancing policy coordination, including through the creation of the Hybrid Centre of Excellence (Hybrid CoE) and the subsequent Joint Declarations and Progress Reports that began in 2016. This development is part of a wider change in the logic of security governance. Rather than reacting solely to active threats, NATO and the EU are conducting proactive resilience measures in order to safeguard societies against cognitive and informational manipulation. This plan does not only include hardening critical infrastructures, but also strengthening public trust, media literacy, and democratic cohesion. In these regards, disinformation is not only a by-product of hybrid conflict, but it is directly used as a primary mean of assessing liberal democracies adaptability.

To conclude, hybrid threats and disinformation are becoming a strategic prioritisation of both NATO and the EU which implies a significant shift in how the security problem is perceived and the manner is addressed. Despite the deepening and improvement of doctrinal recognition and institutional cooperation, the complexity of the current hybrid threat landscape, and especially those involving information dimensions, continues to overload the existing security paradigms. Therefore, having now outlined why hybrid threats and disinformation have become strategic priorities for both NATO and the EU, and how institutional interdependence shapes their responses, the following chapter turns its focus to NATO's approach. It deepens how the Alliance has incorporated disinformation into its strategic thinking, with particular attention to the doctrinal, communicative, and operational adaptations made during the COVID-19 pandemic.

Chapter 2. NATO's approach to Hybrid Threats

Over the past 15 years, the North Atlantic Treaty Organization (NATO) has been compelled to adjust its strategic framework to the changing security environment increasingly dominated by hybrid threats, specifically disinformation. What used to be considered a secondary concern has now become a central priority of the strategic agenda of the Alliance. Since the spread of disinformation has been leveraged by adversaries, many of whom are state actors including Russia and China, to undermine democratic institutions, destabilize governance, and manipulate public discourse, NATO has recognized the need to evolve beyond its traditional military-centric approach into a comprehensive approach to the future of hybrid warfare.

The discussion that follows examines NATO's evolving response to disinformation as a strategy to counter hybrid threats. It explores the Alliance's conceptual and institutional shift from focusing on conventional military deterrence to integrating cognitive security and non-kinetic means in its strategic framework. At the centre of it, there are three interconnected factors: NATO's early recognition of hybrid threats, its doctrinal adaptations to incorporate disinformation as a strategic issue, and the enduring institutional challenges that hinder the Alliance's ability to effectively combat disinformation that can be seen as obstacles to the capacity of institutions to confront disinformation, such as technological disruptions, political fragmentation within the Alliance, and resource limitations (Milo, 2021; de Maio, 2020).

The chapter also analyses three landmark experiences of NATO's counter-disinformation process, each marked by a Summit: the 2014 Wales Summit, the 2016 Warsaw Summit, and the 2022 Madrid Summit are examined to track the Alliance's attempts to address the disinformation issue and, simultaneously, reveal the inherent deficiencies in its counter-disinformation structure (NATO, 2022). The argument is that despite its significant progress in incorporating disinformation into its hybrid threat strategy, achieving long-term success will depend on deeper inter-sectoral coordination, enhanced political unity among Member States, and a strategic recalibration making resilience against information manipulation a pillar of collective defence.

In answering the question of what NATO is doing in terms of its approach to disinformation, the discussion will rely on the two theories that guide the whole research: Hybrid Threats Theory (HTT) and Resource Dependence Theory (RDT). The main issue, which HTT recognises with regards to hybrid threats is their ability to integrate both conventional and non-traditional tactics

to create ambiguity and confusion. The framework therefore suggests that NATO needs to develop its toolbox to combine both military and non-military measures, emphasizing the importance of information resilience in a rapidly changing security environment. RDT, on the other hand, highlights the dependence of NATO on external partnerships especially in the realm of technology and information. Since the Alliance lacks the regulatory and informational capabilities to address disinformation independently, it relies on other players, such as the European Union and private tech companies, to fill these gaps (Anagnostakis, 2025).

To provide a clear and structured understanding of NATO’s evolving approach, the following timeline gives an overview of the key milestones and doctrinal shifts that have shaped the Alliance’s response to hybrid threats and disinformation. These chosen events are doctrinal and operational turning points that have led to the response of the Alliance to counter hybrid threats and disinformation. This visual storyline shows not only significant successes but also captures the remaining problems as NATO keeps refining a strategy in response to the ongoing challenges in the current hybrid threats environment.

Table 1: NATO’s Evolution in Response to Disinformation and Hybrid Threats

Year	Key Event / Initiative	Significance
2014	Annexation of Crimea	Marked a turning point; disinformation recognised as a hybrid threat targeting NATO members.
2016	Warsaw Declaration	NATO formally acknowledged hybrid threats, including disinformation, in its strategic documents.
2017	StratCom CoE	Dedicated centre to coordinate strategic communication and counter disinformation efforts.
2018	Cyber Defence Pledge	Enhanced cooperation on cyber and information security, integrating disinformation countermeasures.
2020	COVID-19	NATO adapted its communication strategy to address the surge of pandemic-related misinformation.
2023	Increased collaboration	Formal steps taken with EU to share intelligence and coordinate responses to hybrid threats, including disinformation.

Source: Author’s own elaboration based on NATO official documents

This chronology marks the process by which NATO has come to recognize disinformation as a central security challenge and illustrates the incremental institutional changes made to address it. However, it also reveals persistent gaps in coordination, political consensus, and resource allocation that must still be addressed to enhance the Alliance’s overall resilience. The following sections take a closer look at the specific strategic adaptations, operational initiatives, and partnership dynamics that characterise NATO’s current stance on hybrid threats and information warfare.

2.1 NATO responses to Hybrid Threats

The first NATO's engagement with hybrid threats was significantly influenced by the 2006 Israel–Hezbollah conflict that revealed the ability of non-state actors to blend conventional military strategies with irregular tactics and information warfare. This episode highlighted the value of asymmetric warfare in which adversaries use the combination of kinetic and non-kinetic methods to achieve strategic objectives below the threshold of conventional armed conflict (Colom Piella, 2022; Biddle & Friedman, 2008). Moreover, it revealed a fundamental flaw within NATO's conceptualisation of hybrid threats: a failure to understand the long-term impact of information warfare as an integrated element of a wider military strategy. As a result, NATO's satisfactory strategic response was delayed, which was evident in the lack of immediate doctrinal reforms post-2006.

Recognizing the changing threat landscape, NATO began to readjust its strategic focus, a shift that became evident in the 2008 Bucharest Summit Declaration which emphasized the Alliance's need to prepare against emerging non-traditional threats. The 2007 cyberattacks on Estonia, widely attributed to Russian-aligned actors, provided a critical wake-up call for immediate action. The attacks targeted the government, banking, and media systems in one of NATO's Member States, revealing the vulnerability of democratic societies to cyber-enabled hybrid operations. Through the lens of HTT, these cyberattacks demonstrated that NATO struggled to conceptualise and counter hybrid tactics that operated in the cyber and information warfare space instead of the conventional military operations. This incident triggered NATO's formal acknowledgment of hybrid warfare as a strategic issue and to include hybrid threat dimensions in planning sessions, such as the 12th Capabilities Planning Review and the long-term strategic foresight efforts like the Multiple Futures Project (Colom Piella, 2022). Nevertheless, the practical effects of these shifts remained largely under-theorised in formal doctrine, reflecting institutional resistance to fully incorporating non-kinetic forms of warfare into its long-established military-centric framework.

Regardless of these emerging dynamics, hybrid threats continued to be underrepresented in NATO's formal doctrine. As an example, the 2010 Strategic Concept acknowledged cyber threats, terrorism, and transnational crime as emerging challenges but failed to explicitly address disinformation or information warfare as strategic issues (NATO, 2010). Such omission reflected not only a reluctance to prioritize non-military forms of aggression but also pointed out a deeper

institutional failure to recognise the evolving nature of modern warfare, in which non-kinetic threats contribute as much as kinetic ones. This formed a conceptual lacuna that left NATO poorly prepared to tackle new forms of hybrid threats that defied the traditional war-peace dichotomy, exposing the institutional limitations in its conceptual frameworks.

A significant shift occurred in 2014 following Russia's annexation of Crimea. The operation featured a sophisticated use of hybrid tactics, combining cyber operations, covert troop movements, and an expansive disinformation campaign that leveraged state-controlled media outlets such as RT and Sputnik to disguise Russia's involvement and destabilize Ukraine. This narrative of the Kremlin not only wanted to legitimize its aggression but also aimed to weaken the cohesion of NATO Member States (Chłóń, 2022). These tactics had such strategic implications that an emergency meeting was held under Article 4 of the North Atlantic Treaty, only the fourth in NATO's history, which reflected the Alliance's elevated concern regarding hybrid threats (Statement by the North Atlantic Council, 2014). This moment serves as an example of why hybrid warfare can alter NATO's strategic priorities, forcing the Alliance to confront the fact that traditional deterrence models were insufficient to counter these complex, interconnected threats.

As a reaction to this, NATO started to reframe its strategic framework. Disinformation, once considered a peripheral issue, was integrated into its hybrid threat response. The so-called "Gerasimov Doctrine", commonly referred to as the Russian model of integrated warfare, further emphasized the blurred lines between conventional and unconventional operations, pushing NATO to reconsider the boundaries of security strategy (Bērziņš, 2020). With the development of NATO's strategy, the focus on cognitive resilience and strategic communications grew in importance and became an essential tool to employ against hybrid threats. In this regard, Rühle (2021) states that "NATO's reaction towards hybrid threats has significantly evolved since 2014, with these elements becoming core pillars of its overall strategy". This change reflects an increasing of NATO's awareness on the measures to deal with hybrid threats, which are not merely a traditional military matter of deterrence or defence; rather it is a perception and safeguarding of the integrity of the information environment. By incorporating cognitive resilience, NATO sought to strengthen societal resistance to disinformation and other forms of malign influence, which demonstrates the multidimensional, cross-sectoral nature of hybrid threats response. This development also brought out the shortcomings of NATO's historically

military-centric framework, particularly when dealing with challenges that require civilian expertise, such as information warfare. NATO summits that followed in Wales (2014), Warsaw (2016), Brussels (2018), London (2019), and Madrid (2022), sequentially expanded the hybrid threat agenda to include strategic communications, resilience-building, and cognitive security initiatives (NATO, 2022).

Through Hybrid Threat Theory (HTT) and Resource Dependence Theory (RDT), a rigorous analysis of NATO's evolving strategy to address hybrid threat can be put in perspective. NATO is increasingly dependent on civilian cooperation to address non-kinetic threats, such as disinformation and cyber warfare, as it needs to adapt its military-centric focus to the growing civilian expertise requirements. Such transparency is an indication of NATO's institutional vulnerability, particularly to its traditionally military focus, and now it must cooperate with external entities like the EU to address institutional jurisdictional gaps regarding media regulation and digital governance. RDT sheds light on this growing interdependence on external partners while revealing the limitations of its traditional military framework in addressing hybrid warfare. As Anagnostakis (2025) points out, "NATO requires strong partnerships with organisations that possess complementary capabilities, particularly in the civilian sphere".

Taken all these together, NATO's strategic posture has undergone a fundamental transformation as it moved beyond traditional military defence and started acknowledging the complexities of hybrid warfare. While NATO's adaptation has been significant, the challenge to fully integrate non-kinetic dimensions into military structures remains an ongoing concern. The following section examines how NATO's growing understanding of disinformation has shaped its strategies, revealing further dimensions of its evolving response to hybrid threats.

2.2 NATO's recognition of Disinformation as a Hybrid Threat

At the Wales Summit in 2014, NATO adopted an official definition of the concept of hybrid threats by putting disinformation at the forefront of its security discourse and aligning with the current academic debate on security threats. During a meeting, NATO's Secretary General, Jens Stoltenberg, characterised hybrid threats to be "the dark reflection of our comprehensive approach," which places them as forces of disruption in the Euro-Atlantic area (Colom Piella, 2022). This new conceptual innovation reveals that the Alliance is aware of the multidimensional nature of modern threats and its increasingly dependence on non-kinetic tools, including

disinformation, cyber operations and information manipulation. In its turn, NATO launched a package of measures that included an improved intelligence sharing and the creation of mechanisms to counter hybrid threats. The convergence of these measures represents a strategic shift towards a more integrated approach to modern warfare, a dynamic in line with HTT disrupting the traditional distinctions between war and peace by stressing the destabilisation of recognition of hybrid threats.

A key outcome of the Wales summit is the establishment of the NATO Strategic Communications Centre of Excellence (StratCom COE) in Riga, Latvia. It is a specialised centre that studies disinformation trends, develops counter-narratives, and supports Member States, which is a clear significant change in the conventional NATO principles. The Alliance is based not merely on military response but also on its reliance on external partnerships and non-military means (NATO, 2014). This kind of dependency resembles the position of RDT which argues that organisational vulnerability is increased through the reliance on external expertise, technology and intelligence. Most recently, partnerships with civilian engagement have extended to combat disinformation and this can be seen with NATO's engagement with StratCom COE and the EU's East StratCom Task Force that was launched in 2015 to monitor and counter Russian disinformation efforts.

In the 2010s, the Tallin Manual organised by the NATO Cooperative Cyber Defence Centre of Excellence greatly changed the direction of the legal and conceptual understanding of information and cyber operations. Though not a validated NATO doctrine, the Tallin Manual on the International Law Applicable to Cyber Warfare (2013) and its expanded Tallin Manual 2.0 (2017) provided key legal interpretations as to how international law applies to cyber operations, including disinformation campaigns. The Manual assessed issues about sovereignty, non-intervention, and the legal thresholds of cyber activities during both armed conflict and in peacetime. Even though disinformation falls into a legal grey zone, the Tallin framework helped NATO to develop a better understanding of cyber-enabled hybrid threats and emphasised the importance of attribution and proportional response in the information domain (Schmitt, 2017). Such focus on non-kinetic aspects aligns with the increased NATO's recognition that hybrid threats are not limited to visible military activity but require new strategic solutions. Moreover, albeit its non-binding character, the Manual remains an influential source in NATO's doctrinal development and has influenced other discussions on international cyber norms.

By the 2016 Warsaw Summit, NATO had institutionalised hybrid threat response strategy, identifying them as “a broad, complex, and adaptive combination of conventional and non-conventional means” (NATO, 2016). This strategy focuses on three pillars: preparedness that focuses on early identification and response, deterrence that is used to strengthen societal resistance, and defence that is used to build rapid NATO response capabilities (Colom Piella, 2022). The Warsaw Summit’s Communiqué explicitly identifies disinformation as an important element of hybrid threats and observes that hybrid attacks can activate NATO’s collective defence clause under Article 5 (NATO, 2016). Hybrid threats are therefore officially characterised as “a combination of conventional and non-conventional means, including overt and covert military, paramilitary, and civilian measures and identified disinformation as a major component of these” (Warsaw Summit, 2016, para. 72).

It was the realisation that disinformation campaigns, when combined with other hybrid tactics, can have strategic consequences to that of conventional military aggression that the 2022 summit shed light on. Stoltenberg (2020) in his #NATO2030 speech emphasised that “strengthened political resilience and better narrative coherence is required”, thus showing that NATO now perceives disinformation, cyber operations and military actions as an integrated effort at destabilising adversaries and undermining societal cohesion. Hybrid threats are therefore not simply merely a mix of military and civilian tactics; they represent a comprehensive approach to warfare comprising of the military, cyber, legal, and informational domains, which act simultaneously. However, the integration of disinformation as a key principle of NATO’s strategy presents new challenges. HTT examines how these tactics like disinformation, cyber operations, and military actions, are often seamlessly combined into a single, coherent strategy which further complicates NATO’s response as interdisciplinary threats require close cooperation of the military, legal, cyber, and civilian domains. The ability of the Alliance to effectively counter these threats is also hindered by its need to coordinate across sectors thus highlighting the increased significance of cross-sector collaboration and political unity.

The summit also saw the launching of NATO’s Counter Hybrid Support Teams, which assist Member States to identify and respond to hybrid threats. It is one of the efforts that NATO has undertaken to increase focus on the need to operate in a cross-sectoral cooperation that is very necessary in the fight against hybrid threats. Simultaneously, NATO and the EU have an

intertwined relationship whereby the latter, regularised in the 2016 Joint Declaration including 20 joint proposals, relies on the former to further collaborate on areas of strategic communications and disinformation resilience, indicating that the alliance has become more dependent on outside knowledge (Flipec, 2021). Despite this, researchers like de Maio (2020) and Milo (2021) assert that NATO's reactive posture and internal political constraints, driven by the need for consensus among Member States that have discrepant threat perceptions, often prevents rapid and coordinated action that would be necessary to effectively respond to modern hybrid challenges.

In the late 2010s, NATO had formulated a more proactive approach to hybrid threats, including disinformation. The same was reaffirmed at the 2019 London Summit where it was emphasised that improving public diplomacy is key to countering hostile narratives and perfecting messaging by the Alliance itself. At the same time, NATO launched the so-called "Setting the Record Straight" initiative, a rather progressive step that aims to actively debunk false claims and promotes fact-based narratives (NATO, 2019). The initiative further pointed out that the focus of the Alliance had now also expanded beyond Russia, as the increasing role of China in disinformation campaigns emerged as major issue of concern. Lastly, the London Summit Communiqué stated that increased coordination between the allies is necessary to address the emerging threats within the information domain (NATO, 2019).

Further on, the COVID-19 pandemic once again demonstrated the risks brought about by disinformation. During the crisis, Russia and China took it as an opportunity to spread conspiracy theories, undermine trust in Western vaccines, and deepen societal divisions (Chłoń, 2022). NATO, in its turn, released the Action Plan for Countering Disinformation on COVID-19 underlining the need to focus on coordinated efforts, fact-checking initiatives, and public awareness campaigns (NATO, 2020). This response demonstrates NATO's evolving ability to adapt to the rapidly changing landscape of hybrid threats, but also revealed its resource dependence, particularly on external civilian actors to counter disinformation effectively.

The 2022 Madrid Summit marked one of the last turning points in NATO's evolving hybrid threat strategy. The new NATO 2022 Strategic Concept was the first document to explicitly recognise that disinformation and cyber operations are a direct security threat to the Euro-Atlantic security and that the Alliance would intensify collaboration with the EU. Interconnectedness with the

European Democracy Action Plan (EDAP) and working closely with the EU's Digital Services Act (DSA), targeting the regulation of the online platforms and mitigation of false information, show how close the connection between NATO and civilian bodies has come in terms of managing hybrid threats (NATO, 2022). Additionally, NATO also made additional enhancements to its intelligence-sharing mechanisms with further cooperation among national cybersecurity agencies to improve early warning systems for disinformation attacks. These measures align with HTT's emphasis on the cognitive dimensions of hybrid warfare, which aim to build public resilience and to better prepare societies to resist the disruptive effects of disinformation campaigns (Genini, 2025).

Overall, recent NATO's treatment of disinformation has evolved to become a key component of its hybrid threat strategy. Institutional reform, legal analysis, strategic planning, and cross-sector cooperation has contributed to this development. However, challenges remain. NATO's limited civilian mandate and the need for political consensus continue to hamper its ability to act with high levels of agility when addressing hybrid threats. The following section will focus in greater detail on these institutional constraints and internal divergences that make NATO's response complicated.

2.3 Institutional constraints and internal divergence in NATO's response

Although the rate of improvement that NATO has taken part of in countering hybrid threats and specifically disinformation, the organisation has so far been faced with numerous challenges which limits the effectiveness in its operations. These issues are grounded in the rapid development of disinformation strategies, the complex process of upholding democratic values in the face of information manipulation and the fragmented approaches among Member States as well as the resource constraints that limit counter-disinformation initiatives. Taken altogether, these elements create serious concerns about the future in NATO's long-term strategic direction and its ability to uphold credibility in a changing threat environment.

One of NATO's primary challenges in addressing disinformation is the fast-evolving nature of information warfare. Adversaries can spread disinformation at an unprecedented level with the increasing sophistication of digital tools. The challenge is further complicated by the emergence of Artificial Intelligence (AI) and deepfake technology that make the detection and debunking of false narratives harder. Malicious actors are increasingly using AI-generated content to create

convincing yet entirely fabricated images, videos, and audio recordings, aiming to mislead the public, manipulate the political discourse, and undermine trust in democratic institutions (Genini, 2025). In terms of HTT, this shift marks the transition to non-traditional warfare, in which the control of the information domain is one of the major strategic goals.

The recent study of NATO on hybrid warfare shows how emerging and disruptive technologies become a deciding factor. According to the 2021 NATO Artificial Intelligence Strategy, AI is a dual-use tool that can be helpful to defence against disinformation while being a weapon in the hands of adversaries. This mutuality resembles the dependency aspect of RDT in which NATO is forced to rely on external technological solutions to solve the challenges it is unable to address on its own. The example of AI-powered bots amplifying disinformation campaigns by generating coordinated social media posts at an increased speed would overload the fact-checkers responding capabilities (NATO, 2021). Simultaneously, deepfake videos are being used to create fake statements from political leaders eroding public trust in institutions and traditional media sources. Likewise, social media platforms have become a battleground for disinformation campaigns and other state actors, such as Russia, have been taken advantage of the algorithmic biases of platforms such as Facebook, Twitter, and TikTok to spread divisive narratives. Therefore, it is necessary to increase collaboration with such platforms to strengthen transparency and accountability of disinformation counteracting efforts underlined by the 2022 Madrid Summit (NATO, 2022). However, NATO's efforts to engage tech companies have not been met with success commercial interests as it not always aligns with the security agenda of the Alliance.

Another challenge that NATO faces is how to balance counter-disinformation efforts without undermining the protection of democratic values like the freedom of speech and media plurality. Compared to authoritarian regimes, NATO's Member States are compelled to conduct their operations in a democratic framework where freedom of expression is prioritised. There is thus a fine line to be crossed between protecting public discourse and avoiding censorship in order to regulate disinformation (Chłóń, 2022). Although NATO has implemented a "pre-bunking" approach that educates the public about disinformation tactics before they take effect, critics argue that it is insufficient to deal with large-scale, state-sponsored disinformation campaigns. HTT suggests that this approach reflects NATO's attempts to manage the cognitive domain of hybrid warfare, aiming to shape perceptions proactively rather than reactively.

The fragmented nature of NATO's counter-disinformation efforts is also a significant obstacle. Though the Alliance generates high-level strategic directions, the implementation of domestic disinformation response is solely to the duty of the individual Member States. The combination of divergence in national policies, varying political will and changing media systems results in inconsistent practices within the Alliance, generating uneven resilience to disinformation (NATO, 2022). Estonia, Latvia, and Lithuania are examples of how a history of Russian influence campaigns has led to a strong media literacy program, state-funded fact-checking initiatives, and rapid-response units debunking disinformation in real-time (Chłoń, 2022). In comparison, other countries within NATO, especially those located in South and West Europe, have taken gradual steps towards the development of national counter-disinformation strategies, thus creating resilience gaps within the Alliance. HTT argues that this fragmentation poses NATO's major dilemma because it reduces the efficiency of the overall strategy. As a result, a high degree of harmonisation at the level of Member States is required to address the challenges of hybrid threats, which prove to be challenging as various national interests are at stake.

Moreover, NATO's counter-disinformation initiatives face financial and logistical constraints. Despite an increasing recognition of disinformation as a significant security challenge, defence budgets and resources remain largely oriented towards conventional military deterrence. As a result, counter-disinformation efforts programmes remain underfunded (Genini, 2025). NATO Strategic Communications Centre of Excellence (StratCom COE) in Riga carries out important work on disinformation trends and develops counter-narratives, but its capabilities are too limited to keep up with the challenge. Building resilience is also within the scope of the activities of the Hybrid Threats Centre of Excellence in Helsinki, yet such activities still rely upon the maintenance of a long-term political and financial commitment of Member States (Hybrid CoE, 2024). These resource limitations point towards a larger strategic culture gap inside the Alliance: the traditional deterrence theory has always favoured visible, kinetic threats that can be countered by proportional force or escalation, whereas a cognitive threat like disinformation does not follow these logics as they are deniable, decentralized, and cumulative in effect. RDT further illuminates NATO's resource challenges, where the reliance on external partnerships, such as the EU and private tech companies, strains its ability to act independently. These gaps weaken the ability to send signal credibility or implement retaliation, both key elements of classical deterrence (Milo, 2021). In this regard, NATO should ensure coordination of its

deterrence approach in the information domain by establishing narrative resilience, public trust, and anticipatory communication strategies as preventive activity against disinformation.

In conclusion, NATO's strategic response to disinformation has transformed significantly over the last 15 years. Although NATO's improvement in developing counter measures has been notable, moving from initial reluctance to engage with information warfare to acknowledging disinformation as a direct security threat, some of its major challenges persist. Such as the necessity to rapidly evolve disinformation tactics, balance security and democratic values, ensure effective coordination among Member States, and address resource constraints. Therefore, the first policy priority is the increase in public resilience, prioritising investments in strategic communications, as well as the integration of new technological tools to address emerging threats. All while preserving freedom of speech and democratic principles, which are inherent to the Western liberal order (Chłoń, 2022). To safeguard democratic societies against information warfare, NATO needs to be dynamic and preventive in the face of changing hybrid threats.

The following chapter analyses the strategic response of the European Union against hybrid threats, one of the areas where the Union installs regulatory, legal and societal tools to counter disinformation. Such institutional asymmetries provide a basis of potential complementarity and of possible friction, especially in the broader transatlantic approach to hybrid threats.

Chapter 3. EU's strategic response to Hybrid Threats

Over the past few years, disinformation has evolved into a widespread threat to the public information environment, thus threatening democratic governance, societal cohesion, and international security. In the European Union (EU), organised Foreign Information Manipulation and Interference (FIMI), especially those driven by authoritarian leaders like Russia and China, have demonstrated the fragility of liberal democracies and weakened the trust in its institutions (Berzina et al., 2019). These disinformation campaigns taking place in the grey zone between war and peace exploit the digital platforms and institutional vulnerabilities to build narratives and weaken the EU's normative legitimacy (Van Raemdonck & Meyer, 2024).

Disinformation has emerged not only as a media issue, but also as a tactical element within broader hybrid threat campaigns, which seek to target democratic weaknesses through information warfare, digital manipulation, and political interference. Due to this, the EU has progressively employed a multi-dimensional approach that encompasses external action, legal frameworks, and societal resilience. Such a trend can be questioned on the basis of Hybrid Threat Theory (HTT) and Resource Dependence Theory (RDT). HTT theorises disinformation as an independent, non-kinetic measure to be deployed in parallel with the multi-domain conflict, and RDT highlights the EU's reliance on private digital platforms and Member State cooperation as critical but often externally controlled resources.

Although EU measures contain features of normative coherence and multilateral governance, they are best understood in terms of the presence of cross-domain vulnerabilities in HTT and through the perspective of operational interdependence in RDT. There have been multiple institutions that have worked within the centre, particularly the European External Action Service (EEAS), the East StratCom Task Force, and the European Digital Media Observatory (EDMO) with the cross-sectoral initiatives including the European Democracy Action Plan (EDAP) and the Digital Services Act (DSA) (EEAS, 2021; EDMO, 2023). Taken together, these approaches have both the aim of detecting and debunking hostile narratives while also empowering civil society and building long-term democratic resilience. A timeline of the main points in history of the EU's strategic approach to disinformation is provided below, which clarifies the integration of policy, regulation, and operational tools over the years.

Table 2: Timeline of the EU’s Strategic response to Disinformation

Year	Key Event / Initiative	Significance
2015	East StratCom Task Force	Focused on countering Russian disinformation and enhancing the EU’s strategic communication capacity.
2016	EEAS Response	Launched rapid response mechanisms to counter hybrid threats including disinformation.
2018	Action Plan	Comprehensive policy framework enhancing platform accountability, transparency, and cooperation with member states.
2019	DSA proposal	Regulatory effort aimed at curbing harmful online content and enhancing transparency.
2020	COVID-19	Coordinated EU-wide initiatives to counter pandemic-related FIMI campaigns and reinforce cross-border strategic communications.
2023	Strengthened collaboration	Joint declarations and working groups with NATO established to build shared resilience against hybrid threats.

Source: Author’s own elaboration based on EU official documents

The European Union has been committed to build a robust, multi-faceted response to disinformation amid the broader hybrid threat landscape. Its evolving engagement can be traced with the previous table, which highlights the subsequent policy evolutions and the cooperative mechanisms that have been critical to this effort, while also pointing out the ongoing weakness of coordination, enforcement, and the balance between regulation and safeguarding democratic freedoms.

Thus, the chapter explores the EU’s evolving response to counter hybrid threats by focusing on the architecture of its disinformation strategy, the operational role of strategic communication tools, and the resilience-enhancing mechanisms developed pre- and post-COVID-19 pandemic. It starts with a description of institutional frameworks and continues to assess the pandemic as a stress test revealing both institutional strengths and critical limitations in terms of adaptability for the EU. The chapter wraps up by evaluating permanent divides and tensions, between regulation and rights, unity and fragmentation, which persist to limit the ability of the Union to respond rapidly to the evolving hybrid threat environment. The Hybrid Threats Theory (HTT) and the Resource Dependence Theory (RDT) is the analytical framework used to evaluate the strategic logic, institutional constraints, and interdependencies shaping the EU’s counter-disinformation approach.

3.1 The EU's frameworks against Disinformation

The European Union's institutional response to deal with disinformation has evolved to a multi-layered system grounded in the use of diplomacy, regulation, strategic communications, and public resilience. HTT reflects the way the EU is addressing the hybrid nature of disinformation threats, as it targets vulnerabilities across multiple domains simultaneously, including foreign policy, cybersecurity, internal market regulation, and democratic governance. RDT, on the other hand, justifies the Union's approach which favours multilateral rules, democratic oversight, and functional cooperation across sectors, focusing on safeguarding the information space in a manner that it does not undermine key fundamental rights like freedom of speech and media pluralism (Raemdonck & Meyer, 2023).

Prior to 2015, the EU had not developed a coherent institutional response to disinformation; the issue was largely treated as a marginal concern within broader discussions on media regulation and foreign policy, without dedicated structures or a strategic framework. As Cullen (2021) points out, this gap in early warning systems left the EU vulnerable to coordinated information operations by foreign actors, making the union particularly susceptible to the kinds of hybrid threats that HTT identifies, which are those exploiting multi-domain vulnerabilities. As a result, the EU was left vulnerable to coordinated information operations by foreign actors, revealing the type of capability asymmetry that HTT seeks to explain.

After the March 2015 European Council conclusions, the EU initiated an institutional response to disinformation by creating the East StratCom Task Force under the European External Action Service (EEAS). Created to address the Russian propaganda targeting Ukraine and the EU's eastern neighbourhood, the Task Force emerged as a key reference point in both detecting and refuting the pro-Kremlin propaganda as disinformation was increasingly understood as a hybrid threat that could achieve strategic goals without direct military confrontation. EUvsDisinfo is a flagship project launched by the EU that maintains a public database of false claims and disseminates evidence-based content to counter FIMI (European Council, 2015; EUvsDisinfo, 2023). Consequently, this project plays a central role in identifying and debunking pro-Kremlin disinformation narratives.

Nevertheless, Cullen (2021) observes that the early orientation of the Task Force was rather reactive since an integrated early-warning system was lacking, which made the EU vulnerable to

rapidly evolving disinformation efforts, underscoring the need for a more proactive strategy. Over the years, the Task Force expanded its scope to include other malign actors, including China and Iran. By the time of the COVID-19 pandemic, its monitoring intensified, especially regarding the disinformation on matters of public health. These trends depict a process of institutional response to changing hybrid threats and highlights the EU's dilemma to maintain operational capacity over an increasingly complex and rapidly dynamic environment, a key aim of the HTT framework due to multi-domain vulnerabilities. As of 2023, the EEAS introduced a structured methodology to detect and attribute FIMI campaigns, which contributes to the strengthening of its operational capacity (EEAS, 2023).

Strategic communication was an initial pillar of the EU responses to disinformation, but gradually it became more evident the need for regulatory intervention. The 2018 Code of Practice on Disinformation brought the first attempt to engage digital platforms such as Facebook, Google, Twitter, and TikTok through voluntary commitments on transparency, demonetization of false content, and fact-checking cooperation. Independent assessments and internal reviews made by the European Commission in 2021, though, affirmed that that these voluntary mechanisms were characterised by a lack of consistency, enforcement, and effectiveness (European Commission, 2021).

According to Cullen (2021), the absence of an integrated early warning system did not allow the EU to accurately anticipate the extent of the emerging disinformation campaigns, which made it more difficult to respond effectively in time. Such deficiency of anticipatory capacity demonstrates a conventional problem of RDT: institutional resilience on private platforms, which was essential, did not provide the overall retaliation to effectively suppress disinformation. As a reaction, the EU proposed the Digital Services Act (DSA) in 2022, a regulatory milestone that binds Very Large Online Platforms (VLOPs) to a set of obligations. The DSA mandates risk assessments when dealing with algorithmic amplifications and increases transparency in content moderation and formal cooperation with national regulators. Thus, it strengthens the EU's global leadership in the governance of digital information environments (European Commission, 2022; Van Raemdonck & Meyer, 2024). The shift to a compulsory over voluntary regulation is an indication that the EU wants to minimise institutional reliance through legal control of platforms but also wants to counter the vulnerabilities encountered in the hybrid threat environment.

In line with addressing regulatory reform, the EU has also focused on societal resilience through the European Democracy Action Plan (EDAP), which was adopted in 2020. The EDAP develops a detailed vision of countering disinformation and protecting democratic norms. It promotes media pluralism, transparency in political campaigning, and civic education aimed at enhancing digital literacy. Within this framework, a key component is the European Digital Media Observatory (EDMO), a decentralised network of fact-checkers, academic researchers, journalists, and media literacy practitioners. The EDMO is used to support cross-border collaboration, methodological standardization, and evidence-based policymaking in order to overcome disinformation effectively (European Commission, 2020; EDMO, 2023).

The recent interest on building societal resilience within the EU comprehends the level of understanding that cognitive security does not lie in regulatory remediation that simply address the root causes of vulnerability that are intrinsic in the democratic discourse. This orientation is part of a broader strategy of the EU to mitigate the multidimensional nature of hybrid threats by increasing societal immunity. In spite of the fact that EDMO carries out the central role of promoting public resilience, the integration of early warning systems into this framework remains a significant challenge. According to Cullen (2021), the EU's current structure has no foresight ability that can combat disinformation, especially given that the threats are evolving across multiple domains. Filling this gap will become necessary so that the EU can address emergent hybrid threats even before they escalate, hence necessitating the need to improve its anticipatory capacity. Improved early warning systems are essential to protect societal resilience by detecting and mitigating disinformation campaigns before they spread.

All in all, the EU's disinformation framework is supported by three strategic pillars: external action and public diplomacy (e.g., East StratCom Task Force), legal and regulatory instruments (e.g., Code of Practice, DSA), and societal resilience (e.g., EDAP, EDMO) all of which reflect the Union's effort to a comprehensive response that aligns with HTT's recognition of multi-vector nature of modern threats. However, the use of RDT helps to demonstrate that the capacities among ongoing digital platforms and of the different Member States complicate the achievement of coherent and rapid responses.

In the sections that follows, it will be emphasised the fact that although the framework represents normative ambition and strategic innovation, it also has uneven performance among the Member States. The jurisdictional and structural intricacies slow down the EU's ability to respond coherently and rapidly to multidimensional hybrid threats, thus showing the ongoing dilemma on how to adopt an effective defence to address the modern security paradigm.

3.2 Strategic communication and resilience tools

The COVID-19 pandemic was a decisive challenge to the European Union's institutional capacity to combat sophisticated forms of information manipulation. Disinformation rapidly became a tool of hybrid warfare, and its malign actors, mainly Russia and China, took advantage of the public's fear, social fragmentation, and institutional vulnerability. Such campaigns align with most essential presuppositions of HTT since they intentionally blur the lines between foreign interference, public health crises, and democratic trust erosion. As explained by HTT, they did not only want to spread falsehoods but to exploit vulnerabilities in the open society structure and discredit democratic institutions, undermining trust in public health responses, and eroding transatlantic solidarity using conspiracy theories and vaccine misinformation (Raemdonck & Meyer, 2025).

The EU stepped up its strategic communication infrastructure when faced with the rapid spread of hostile narratives. In this context, the European External Action Service (EEAS) took a leading position in revealing disinformation narratives, via the East StratCom Task Force and its EUvsDisinfo project, in particular those that circulated through Kremlin-backed outlets such as RT and Sputnik. The initiative catalogued and publicly debunked falsehoods of alleged bioengineering of the virus by NATO or West governments having deliberately held back medical supplies (EEAS, 2020; Wiseman, 2021). EUvsDisinfo expanded its monitoring scope and increased public awareness by issuing weekly digests and thematic reports aimed at journalists, researchers, and civil society. This capacity-building is an institutional learning curve that fits within HTT, given that the EU identified the need to respond to cross-border information operations in real-time.

Aligning with strategic rebuttals, the EU intensified enforcement by leveraging new regulatory tools. The Code of Practice on Disinformation and the Digital Services Act (DSA) imposed more structured demands on digital platforms to make their algorithm more transparent, to moderate

their contents, and to publish their data with researchers. From a RDT perspective, these instruments represent the EU's strategic effort to mitigate its reliance on private platforms whose commercial logic often runs counter to the EU's public interest goals. By shifting from voluntary to mandatory frameworks, the EU enhanced its legal and political leverage over Very Large Online Platforms (VLOPs), thereby addressing the power asymmetry that had previously limited effective governance (European Commission, 2022; Berzina et al., 2019).

The COVID-19 pandemic forced the EU to undertake unprecedented diplomatic steps. In March 2022, the Union took the decision to systematically block the broadcast of Russia-based RT and Sputnik on all Member States, citing the role played by the two channels in the promotion of the Kremlin's sponsored propaganda. These foreign policy moves not only made disinformation a media concern but also a geopolitical issue, as HTT's vision on coordinated non-military aggression. It also indicated a definitive turn towards the recognition of manipulated information as a strategic threat and demonstrated the EU's willingness to use foreign policy instruments to sanction disinformation campaigns (Council of the EU, 2022). Simultaneous resilience-building was enhanced through investment in media pluralism, fact-checking networks, and civic education through the European Democracy Action Plan (EDAP). At the centre of it, there's the European Digital Media Observatory (EDMO) that set up interconnected national hubs to facilitate cooperation between researchers, fact-checkers, and media literacy organizations. It enabled rapid analysis of disinformation trends, sharing of best practices and disseminating counter-narratives (European Commission, 2020; EDMO, 2023). The combination of decentralised solutions with an integrated resilience initiatives allowed the EU to fight hybrid threats not only due to regulations but also by reinforcing cognitive security and societal resilience. The institutional fragmentation considered a weakness in both HTT and RDT was partly reduced by this initiative as it helped overcome inter-Member State disparities in media literacy and digital capacity.

Although there have been technological and institutional innovations, a number of structural weaknesses remain which restrict the ability of the EU to approach crisis management in real time. The EU's civilian-led, regulatory response continues to fall short since structural asymmetries persist among states. The high dependency on national-level implementation and private platforms continues to lead to the creation of coordination gaps that can be used by adversaries (Raemdonck & Meyer, 2025).

Overall, the COVID-19 outbreak resulted in a drastic transformation of the EU's strategic communication and resilience toolkit. The formerly fragmented efforts have been consolidated into a more integrated and proactive framework. By employing legal innovation, public diplomacy, and civil society engagement, the Union strengthened its ability to counter disinformation whilst maintaining the liberal democratic values. However, structural interdependencies and jurisdictional asymmetries are exposed to being used against each other by hybrid threats during future contingencies. This concern is thoroughly discussed in the following section.

3.3 Gaps, challenges and opportunities in the EU's Disinformation strategy

In spite of the significant efforts made by the EU to counter Foreign Information Manipulation and Interference (FIMI) by foreign competitors, the capacity of the Union to provide a comprehensive and coherent response remains limited by the complexity of structural, legal, technological, and societal challenges. Such long-term barriers demonstrate the tension between democratic values and the strategic urgency of countering disinformation. From the lens of HTT, these threats portray how adversaries capitalise on systemic vulnerabilities within open democratic societies in order to achieve hybrid coercion effects without direct confrontation. There remain vulnerabilities in regulatory enforcement, Member State cohesion, control on digital platform governance, and societal resilience.

One of the main weaknesses of the EU's disinformation response lies in the limitations of its regulatory framework. In 2018, the latest Code of Practice on Disinformation became an important initial step, as it introduced a voluntary self-regulatory mechanism for online platforms. Developed as a voluntary agreement that promotes transparency, cooperation with fact-checkers, and accountability of harmful content, its voluntary nature and lack of enforceability has been widely criticized for yielding inconsistent implementation and weak compliance among signatories (Van Raemdonck & Meyer, 2024). This regulatory gap can be conceptualised in terms of RDT that emphasizes the EU's reliance on digital platforms' cooperation as an essential source that remains outside the direct control of the EU, and therefore, limiting the Union's capacity to push binding measures effectively. The European Commission went further in the 2022 revision to include a broader range of stakeholders such as advertisers, civil society, and fact-checking organizations. Nevertheless, the updated Code

remained its non-binding nature and relied on platforms' voluntary implementation (European Commission, 2022).

The Digital Services Act (DSA) subsequently partially addressed these deficiencies by imposing binding obligations on VLOPs to carry out risk assessments, build data-sharing protocols to researchers, and establish oversight measures (European Commission, 2020; Van Raemdonck & Meyer, 2024). Yet, challenges persisted in achieving uniform enforcement across Member States, resourcing national authorities, and navigating a fragmented legal landscape. Moreover, the lack of a shared, binding legal definition of disinformation across the EU complicates regulation and provides ambiguity through which malign actors can seek exploitable loopholes in their cross-border coordination (Berzina et al., 2019). Such lack of clarity also affects the institutional integration.

The EU's response is further hampered with the presence of fragmented implementation process across Member States. Countries such as Estonia, Latvia, and Finland have developed advanced national frameworks for strategic communication and resilience due to their geographical closeness to Russia and the historical exposure to disinformation. On the other hand, it is also observed that some of the Member States lack institutional preparedness or political will, often burdened by domestic sensitivities or competing policy priorities (Giussani, 2020). The resulting imbalance generates a patchwork of national policies that undermine the EU-wide consistency and reduces the effectiveness of such collaboration, as highly exposed countries often bear a disproportionate burden to counter disinformation action. HTT suggests that such fragmentation exacerbates EU's vulnerabilities by offering an environment in which hybrid threats flourish once the collective defence framework is fragmented and slow to adapt. This asymmetry undermines the Union's ability to have a united front, thus weakening deterrence and response capacity.

The threat of pollicisation of disinformation frameworks is becoming increasingly acknowledged. In the context of the EU, the use of the term of "fake news" in some state jurisdictions has been used to discredit the voices of opposition or limit freedom of speech, creating a risk that compromises the EU's commitment to freedom of expression and media pluralism (Van Raemdonck & Meyer, 2024). Using this dynamic is a particular concern in countries that experience democratic backsliding, as counter-disinformation measures may be used or adapted

as censorship tools or state propaganda instead. This paradox highlights one of the main dilemmas of the modern hybrid threat environment: the tools which are constructed to protect democratic institutions are often the same ones that threaten to undermine them, creating a self-inflicted legitimacy crisis. RDT also demonstrates that the political players of any society can abuse legal systems to reinforce their power, which is a significant illustration of the interconnection between the institutional needs and political motivations.

Being a normative actor striving to uphold fundamental rights, the EU faces the challenging issue of reconciling countering disinformation while safeguarding freedom of expression. Article 11 of the Charter of Fundamental Rights ensures freedom of information and expression, which may come into conflict with any regulatory efforts that pose risk of restricting the online discourse. Overregulation or opaque content moderation policies may lead to chilling effects, suppressing legitimate political debate and damaging the integrity of institutions (Pamment, 2020). It is further augmented with the notion of “reflexive control,” whereby authoritarian actors are able to cause democracies to act against their own values in self-defeating responses. On these grounds, the overregulation of information can be weaponised to delegitimise liberal institutions and international norms (Giles, 2016; Van Raemdonck & Meyer, 2024). This is a dynamic that demonstrates how HTT understands the strategic use of normative contradictions in democracies by hybrid threat actors to gain asymmetric advantages. Therefore, the EU’s tendency to embrace tools of soft power such as public diplomacy, civic education, and media literacy rather than coercive legal responses, can be deemed to represent both normative commitment and a strategic need of not letting the adversary gain a tactical advantage. However, this cautious stance has the risk of pre-emptive action disallowing rapid, decisive deterrence against fast-evolving influence operations hence a paradigm of friction between principle and pragmatism.

Another weakness is related to asymmetries in ability as the EU’s responses are failing to keep up with the pace and sophistication of malign actors operating online. Their state-backed disinformation campaigns, especially those by Russia and China, regularly use artificial intelligence, bot networks, deepfakes, and micro-targeted advertising to spread their message on a large scale whilst making it challenging to detect using traditional methods (Giussani, 2020; Van Raemdonck & Meyer, 2024). The European Digital Media Observatory (EDMO) and its affiliated national hubs can provide useful evidence aggregation and collaborative response

capabilities, although it is usually hindered due to inconsistencies in funding, diverse national capabilities, and limited interoperability among member hubs. The backing of efforts by the Digital Service Act (DSA) has increased the availability of data provided by major platforms, though it is limited in its scope and heavily dependent on platform cooperation (European Commission, 2022). Furthermore, disinformation has also become widespread in semi-private or encrypted digital spaces, such as messaging applications or closed social media groups, which are inaccessible through traditional monitoring and moderation tools. As a result, EU policy instruments that are designed primarily for public-facing platforms, are not best prepared to address those domains of digital manipulation. In terms of RDT perspective, the EU's technological and informational dependence on external platforms and private actors contributes to critical gaps in addressing complex hybrid threats. Such technological deficit highlights the structural limits to both state and supranational capabilities in responding to rapidly changing digital threats.

In addition to the limitations set by institutions and technology, societal factors have a determinant impact on how successful the EU can be in countering disinformation. Declining trust in political institutions, rising polarization, and persistent digital illiteracy makes populations more vulnerable to manipulation. Without addressing these social drivers, regulatory and technical solutions will remain reactive and limited in scope (Tagliabue et al., 2020).

Hybrid threats have also been represented by the EU on policy documents like the European Democracy Action Plan and the Audiovisual and Media Action Plan that aim to support media pluralism and digital education. These programs aim to build societal resilience by facilitating critical thinking, motivating civic engagement, and increasing fact-checking support (European Commission, 2020). However, their adoption has often been described as fragmented and under-resourced, and strategic planning has mainly been carried out in short-term project cycles. Significant differences are still observed in the educational systems of the Member States regarding the inclusion of digital literacy, whereas the public campaigns frequently lack visibility or long-term effect. At the same time, initiatives aimed at strengthening civil society actors, independent journalism, and trusted information ecosystems are considered secondary to current regulatory discussions. Despite rhetorical commitments, the funding behind such initiatives is often unstable or politically contingent, further making visible a deeper level of resource dependency beyond platforms to the unpredictable Member States support. Unless

there is a significant investment in civic infrastructure, disinformation will keep on exploiting societal divisions and institutional distrust. This dynamic demonstrates one key insight of HTT: hybrid threats address both physical and institutional vulnerabilities but also the social fragmentation and democratic deficits that facilitate them. Based on this, societal cohesion needs to be incorporated into the resilience strategy as a strategic defence.

In spite of these weaknesses, the EU's evolving strategy has brought some tangible, yet limited outcomes. Platform cooperation with the EU has resulted in thousands of accounts being taken down, and the publication of data showing those outlets sanctioned, like RT and Sputnik, further showing signs of improvement (EEAS, 2022; European Commission, 2023). These gains remain however fragile. The findings of independent studies, including the Standard Eurobarometer 97 (European Commission, 2023) and national reports on disinformation risks 2022-2021 (EDMO, 2023) show that people continue to be vulnerable to false information in several EU Member States and public trust in information ecosystems remains fragmented. The Union's initiatives have succeeded in halting the spread of some narratives, but they have not undermined the structural asymmetries that malign actors take advantage of, pointing to the urgent need to introduce effective enforcement tools, a broader civic infrastructure and long-term public engagement strategies. This fact highlights the systemic nature of hybrid threats where tactical successes are dependent on long-term structural reforms that deal with the root causes of vulnerability.

As a result, despite the effectiveness of the strong legal frameworks and normative coherence of EU's disinformation strategy, the EU partly still lacks coherent efficiency. Disinformation penetrates national boundaries and institutional silos faster than the Union's fragmented governance can respond. The combined use of HTT and RDT in the presented analysis demonstrates that structural dependency and institutional fragmentation pose fundamental limitations to the ability of the EU to respond to hybrid threats effectively. Therefore, in order to improve strategic resilience, it is critical to resolve these intertwined theoretical challenges and improve strategic resilience.

This focus outlines the essential requirements of a more cohesive implementation, sustained civic investment, and tighter coordination among Member States, such as including standardised enforcement mechanisms under the DSA, long-term funding pipelines for EDMO hubs, and the

creation of EU-wide digital literacy curricula integrated into national education systems. These issues are even more exacerbated when it comes to transatlantic cooperation, especially with NATO, which will be discussed in the following chapter.

Chapter 4. Case study: NATO-EU cooperation during the COVID-19 pandemic

Based on the analysis presented in the last section concerning NATO and the EU and their current understanding of disinformation as a key element of hybrid threats, the current chapter focuses on a more practical example of disinformation during the COVID-19 pandemic. The pandemic was not only a significant public health crisis, but also a multidimensional hybrid crisis that revealed new vulnerabilities in systems of public communication and institutional coordination. It is this uncertainty, fear and social fragmentation that were exploited by state and non-state actors to pursue information operations with geostrategic nature, that transformed a health emergency into a battle over narrative control and institutional legitimacy.

The COVID-19 pandemic serves as a case study in understanding how the EU and NATO collaborate in combating hybrid threats, particularly disinformation. Unlike the traditional military conflicts that occur kinetically and consider the state actors as the only target, the pandemic created a non-kinetic, cross-sectoral challenge that tested the strength of democratic institutions, the information ecosystems, social trust, and inter-state coordination. The crisis was exploited by hybrid actors, such as Russia and China, in the form of disinformation campaigns carefully aimed to erode public trust in Western institutions, to undermine pandemic responses, and to promote the adoption of alternative, authoritarian models of crisis governance (Milo, 2021; CEPA, 2021). In terms of HTT, the pandemic revealed how malicious actors take advantage of the institutional blind spots by methodically operating on the level of the cognitive domain and thus transforming it into a discourse of confrontation.

Institutional boundaries were further blurred as a result of the crisis. Whereas the task of NATO does not extend to public health, its strategic communication and security capabilities have become particularly relevant when disinformation was turned into a weapon to destroy the Alliance's cohesion and credibility (Missiroli & Rühle, 2020; De Maio, 2020). At the same time, the EU's digital regulation and health coordination powers made it a key component in applying moderation to content, securing platform accountability, and enhancing public trust in scientific communication (European Commission, 2020; Berzina et al., 2019). This overlap emphasised a structural interdependence of the two institutions, a process that can be explained with RDT as both organisations had to collaborate in fields above their respective capacities.

Such convergence in mandates created a unique situation where both institutions had to challenge the common threat landscape at the same time, albeit differently. The case thus allows an evaluation of the way each institution reacted separately and of the level of functional complementarity, strategic coordination, and institutional friction that could be observed in their joint efforts (Raemdonck & Meyer, 2023; De Maio, 2021). Moreover, crisis was a stress test of strategic foresight, institutional agility and normative coherence to both NATO and the EU. The response of the institutions therefore offers useful information on their abilities to coordinate public communication strategies, engage with private-sector actors, and adapt their strategic frameworks in order to address disinformation as a critical dimension of crisis response (Missiroli & Rühle, 2020; De Maio, 2020). It also marked a turning point in institutional awareness on disinformation: it shifted from being a secondary issue to a direct challenge to democratic resilience and transatlantic security (Caceres et al., 2022; Szymański, 2020).

Whereas NATO had already previously identified disinformation as an increasingly significant security threat following Russia's annexation of Crimea in 2014, the pandemic vastly increased the scale and sophistication of information warfare. This change required adjustments in the military, as well as a more cross-sectoral cooperation and cognitive resilience-building. At the same time, the EU shifted towards stronger regulatory intervention by complementing soft coordination through more binding regulatory action and expanding its legal toolkit and civil society partnerships to combat malign narratives. Despite the similarities in challenge that both organisations faced in their implementation process, such as fragmented national approaches, platform resistance, and resource gaps, they also benefited of strategic lessons that can be used in future cooperation.

This chapter explores the role of disinformation as a key component of hybrid warfare during the pandemic. It begins by looking at the strategies, platforms and narratives used by malign actors to include the use of state-sponsored propaganda, AI-generated content, and social media manipulation. It then evaluates the counter reactions between NATO and the EU and how they performed, pointing out their strengths, limitations, and institutional adaptations. Lastly, it measures the degree of operational synergy and strategic learning that is achieved through their collective efforts. Through the dissection of this case, the chapter highlights the changing nature of hybrid threats and the significance of institutional interdependence, digital sovereignty, and cognitive resilience to future transatlantic crisis management.

4.1 Strategic use of Disinformation during the COVID-19 pandemic

The COVID-19 pandemic brought in a multidimensional and dynamically changing security challenge that extended beyond its immediate public health impact. By unveiling serious weaknesses in societies and gaps in institutions, it enabled malign state and non-state actors to coordinate sophisticated disinformation campaigns. These efforts were aimed at undermining social cohesion, erode public trust, and destabilize Western institutions, such as NATO and the EU, by strategically exploiting fear, uncertainty, and the crisis as their means. The current section examines the targeted use of disinformation during the pandemic, outlining the tactics used and major narratives distributed, as well as institutional and technological vulnerabilities that led to the increase in scale of such operations. To fully understand the bigger picture surrounding hybrid threats, neither NATO nor the EU can ignore the broader hybrid threat landscape, as well as evaluate their subsequent responses.

4.1.1 Weaponizing the crisis: exploiting fear and uncertainty

During the pandemic, disinformation efforts sought to take advantage of specific moments of institutional stress and public anxiety, taking advantage of the fluid and uncertain context in order to have the greatest effect. These coordinated attempts were not isolated or random cases of violence; instead, they were strategically timed attacks on societal resilience aiming to cause distrust and confusion as well as weakening the democratic institutions from within. It was the unpredictable nature of the pandemic and the accompanying evolving scientific understanding that created a favourable environment that further amplified fears, manipulate narratives, and deepen political polarization. This practical manipulation of crisis dynamics shows that disinformation is at the same time a strategic tool and also an adaptive tactic in broader hybrid threat frameworks (Hadlington et al., 2020; Tagliabue, Galassi, & Mariani, 2020).

Malign state and non-state actors, particularly authoritarian regimes like Russia and China, took advantage of the uncertainty and institutional overload to propagate multidimensional disinformation campaigns aimed specifically at destabilising NATO and the EU Member States by exacerbating societal cleavages, undermining public trust in governance structures, and deepening political divisions (Ferreira Caceres et al., 2022). In this regard, defence by disinformation occurred, as an armed part of the hybrid conflict, where the narratives promoted were the ones that questioned the credibility of Western institutions, the safety and efficacy of vaccines, as well as the overall effectiveness of crisis response (Hadlington et al., 2020; Genini,

2025). The operations in question, viewed through the lens of HTT, provide an example of how military tools, primarily digital and psychological, can be used to pursue strategic goals in the grey zone between peace and conflict. As a strategical tool, disinformation works at the level of both weakening societal cohesion and as a broader strategy to destroy resilience of democratic societies (Ferreira Caceres et al., 2022; Tagliabue, Galassi, & Mariani, 2020).

Both NATO and the EU recognized very early in the pandemic that disinformation campaigns were taking advantage of the situation, however, attempting to combat these narratives was difficult due to the fast-evolving nature of digital influence operations and the volume of disinformation that was spread across the internet. Although the conventional mandate by NATO has always been on military defence, the pandemic forced the alliance to deal with non-conventional threats like information warfare, especially towards the Russian and Chinese fronts on strategic disinformation campaigns. The EU, which already had been fighting disinformation by running the EUvsDisinfo platform and the East StratCom Task Force, stepped up to keep track, expose, and debunk false narratives that aimed to polarise and divide EU Member States (Ferreira Caceres et al., 2022).

Despite these efforts, malign narratives were already deeply embedded, taking advantage of structural vulnerabilities in communication systems and psychological stress among populations. (Tagliabue, Galassi, & Mariani, 2020). The tactics used by malign actors were numerous: from fake news and manipulated statistics to state-sponsored propaganda and AI-generated content. Such activities intended to mislead but also to confuse, polarise, and exhaust audience, thus minimising their ability to process and trust legitimate information (Hadlington et al., 2020; Genini, 2025).

Overall, the weaponisation of fear and uncertainty in the context of the pandemic highlights the high effectiveness of disinformation to take advantage of crisis conditions, undermine institutional trust and social cohesion, which poses fundamental issues to the resilience of democracies.

4.1.2 State-sponsored propaganda and conspiracy theories

The use of fear and institutional weaknesses turned out to be one of the most successful strategies of the COVID-19 disinformation campaigns. At the beginning of the pandemic,

scientific uncertainty, changing public health guidelines, and an overload of conflicting information created an ideal environment for disinformation to thrive. Within these parameters, HTT explains the tactical arrangements of adversaries to coincide with moments of institutional vulnerability, thus intensifying the psychological effects. This group of actors took advantage of information vacuum to leak false narratives that undermined the legitimacy of governments, NATO, the EU, and other public health-related institutions (Tagliabue, Galassi, & Mariani, 2020). The parallel application of partial truths and misleading claims made it more difficult to debunk disinformation. As an example, stories that exaggerated NATO's struggles in coordinating pandemic relief efforts were intentionally combined with fabricated claims that NATO purposely refused to send medical supplies to weaker Member States (Chłoń, 2022). Similarly, arguments about the ineffectiveness of Western vaccines were published along with legitimate discussions of rare side effects, which significantly boosted the rates of vaccine hesitancy (Hadlington et al., 2020).

State actors took a leading role in planning such campaigns, using government-controlled media, cyber operations, and shadow networks of influence to destabilise NATO and EU's trust. The Russian-backed outlets like RT and Sputnik posted all kind of statements, that NATO used the pandemic to strengthen its military presence, that the Western countries were gathering up medical supplies and that its vaccines were unsafe. Meanwhile social media bots and troll farms amplified these messages and targeted the groups that were already sceptical of government actions (Genini, 2025). The Chinese state media, such as Xinhua and the Global Times, first attempted to redirect blame on the origins of the virus by perpetrating claims that COVID-19 was originated in a US military research facility; they later shifted towards a more appealing rhetoric that highlighted the success of controlling the virus, high levels of humanitarian assistance, the superiority of Chinese vaccines and criticised Western handling of the pandemic (Hadlington et al., 2020). These tactics made it harder to distinguish between misinformation, unintentional falsehoods, and disinformation, deliberate manipulation, making it difficult to respond institutionally in a timely manner (Ferreira Caceres et al., 2022).

Conspiracy theories are effective tools of discrediting Western institutions. Among them is the hypothesis that COVID-19 is a "NATO bioweapon" (Genini, 2025), the "Great Reset" theory that alleges elite dominance through COVID-19 (British Academy, 2021), and false claims that vaccines have embedded microchips or caused infertility, which makes vaccination discouraging

and fuels the prolongation of the crisis (Ferreira Caceres et al., 2022). These theories thrived in online echo chambers, and where both primed by confirmation bias and selective exposure and also proved resistant to debunking as it would be seen as part of an alleged “cover-up” (Headington et al., 2020). Though these narratives it is demonstrated how strategic planning of the disinformation campaigns aimed to undermine institutional credibility and societal trust to weaken Western cohesion. In response to this, state-sponsored propaganda and conspiracy theories were defined as deliberate tools of hybrid influence, as they exploited pre-existing uncertainties to delegitimise Western institutions and fracture public consensus.

4.1.3 Technical amplifiers: social media, bots and AI

The digital information ecosystem the premises of success of COVID-19 disinformation campaigns. Social media platforms, which were designed specifically to maximize user engagement rather than verify the accuracy of content, inadvertently amplified misleading narratives (Hadlington et al., 2020). Algorithms give preference to sensational, emotionally charged, or polarizing content, which creates a situation when disinformation spreads faster and on a broader scale than factual information (Vosoughi, Roy, & Aral, 2018). This engagement-driven amplification becomes a perfect way to weaponise platform mechanics when it comes to strengthening social divisions and erode trust (Lazer et al., 2018).

Automated bot networks were used to boost disinformation content artificially, thus creating the impression that false claims had prevalent public support (Genini, 2025). In addition to increasing the quantity of the misleading content, troll farms have also managed to manipulate perceived consensus by exploiting the social proof heuristics, which substantially influence the public perception as well as their behaviour (Shao et al., 2018). In the meantime, developments in AI created deepfake videos in which statements by NATO officials were distorted, suggesting acknowledgements of failure or contradictions in their earlier policies (Chłóń, 2022). Beyond deepfakes, advancements in synthetic media such as AI-generated text and imagery, lowered the barriers to creating convincing but fabricated content, making real-time authenticity verification more difficult (Citron & Chesney, 2019).

Coordinated hashtag campaigns such as #NATOFailedEurope and #VaccineDanger were strategically engineered to cause controversy and erode trust in the existing public health recommendations (Ferreira Caceres et al., 2022). These efforts describe how information

manipulators use online viral trends and hashtag activism to infiltrate the public discourse and strengthen polarizing narratives across different digital communities (Starbird, 2017).

The tactical convergence of these strategies effectively unlocked cognitive biases such as confirmation bias and the illusory truth effect, further increasing the speed of disinformation and slowed the spread of corrective information (Tagliabue, Galassi, & Mariani, 2020). Confirmation bias leads individuals to favour information that aligns with their existing beliefs, while the illusory truth effect causes repeated exposure to false claims to increase their perceived accuracy (Lewandowsky et al., 2017; Pennycook et al., 2019), both of which are exploited by disinformation actors to embed misleading narratives deeply in public consciousness.

Once false narratives gained traction, fact-checking efforts struggled to contain their influence, hindered by the speed and scale of disinformation dissemination and the fragmented nature of digital platforms (Tagliabue, Galassi, & Mariani, 2020). Confirmation bias makes people favour information that agrees with their prior views, whereas the illusion of truth phenomenon makes it seem like false statements are legitimised after repetition; both functions are used by propaganda agents to damage narratives into the minds of the masses (Ferreira Caceres et al., 2022). To that end, the current digital information ecosystem becomes a dangerous transmission mechanism of hybrid threats, where technological amplification, psychological manipulation, and geopolitical strategic objectives overlap. Institutional countermeasures, therefore, cannot merely focus on tactical reactivity but also towards understanding and countering of these digital dynamics.

4.1.4 Institutional vulnerabilities: crisis communication and trust deficits

Considering the acknowledged severity of these disinformation campaigns, NATO and the EU developed a number of counter measures to face malign influence operations. NATO founded an initiative to understand and combat psychological manipulation in hybrid warfare called the Cognitive Warfare Initiative (Genini, 2025) and the EU strengthened the EUvsDisinfo Task Force, which methodically monitors, reveals, and debunks disinformation campaigns related to COVID-19 (Ferreira Caceres et al., 2022). Both organisations increased cooperation with social media platforms to encourage taking substantive measures like removing false information, demoting misleading content, and promoting credible sources (Hadlington et al., 2020).

Despite the shared efforts of the international community to respond to issue of misinformation, the spread of COVID-19 disinformation led to far-reaching implications on public trust in governments, health organizations, and international organizations. These campaigns caused political polarisation, increased the unwillingness to take the vaccine and undermined the effectiveness of crisis response by spreading doubt on institutional motivations and competences (Ferreira Caceres et al., 2022). As shown by RDT, NATO and the EU are no exception to the vulnerability against platform-driven dynamics: they are relying on privately owned social media platforms to communicate and implement their policies, and such motives are usually not aligned with the promotion of democratic governance.

The decentralized and evolving nature of disinformation contributes to its difficulty to be fully eradicated, and as the pandemic showed, continuously changing disinformation tactics makes resilience-building a long-term necessity (Tagliabue, Galassi, & Mariani, 2020). These campaigns disoriented the information environment and revealed gaps in crisis communication and digital infrastructure at the same time. As threats evolved, it was clear that a coordinated, institutional-level response was essential.

Overall, the disinformation campaigns surrounding the COVID-19 pandemic actively targeted psychological, technological, and institutional vulnerabilities in order to undermine the crisis management capacity of both NATO and the EU. Such operations exposed massive weaknesses and highlighted the necessity of a strategic and operational adjustments within the two organizations. In this context, the pandemic helped to illustrate how essential is to enhance resilience to hybrid threats by addressing the issues linked to crisis communication, digital infrastructure, and institutional trust. The section below evaluates NATO and the EU's responses in managing the hybrid threats, especially focusing on the institutional agility and the structural limitations which formed their capacities to manage disinformation.

4.2 NATO-EU responses: diverging logics, complementary strategies

The COVID-19 pandemic triggered a rather severe disinformation crisis and to face and overcome this challenge, NATO enhanced its counter-disinformation capability by developing and executing its official document, NATO's Approach to Countering Disinformation: a focus on COVID-19 (NATO, 2020). The document placed disinformation into a wider strategic hybrid warfare

framework and recommended that it be systematised and integrated into the strategic communications structure of NATO. Although such measures were built on the current alliance initiatives, the document additionally emphasises the importance of adapting responses to the rapidly evolving tactics used by malign actors. In parallel, the EU offered complementary countermeasures by mobilising institutions and digital policy frameworks to limit the spread of misleading narratives. As a combination, the security-based focus of NATO and the regulatory measures of the EU display various yet overlapping responses through which the Western institutions are dealing with hybrid threats. Whilst both actors achieved measurable successes, ongoing weaknesses in resilience and coordination highlight the complex nature of countering disinformation in democratic societies.

4.2.1 NATO's strategic response to COVID-19 Disinformation

The counter-disinformation strategy that NATO developed in the pandemic era included multiple elements such as strategic communications, fact-checking initiatives, and partnerships with member states and digital platforms. The four core areas of focus of the Alliance were strengthening strategic communications, reinforcing fact-checking capabilities, enhancing external partnerships, and integrating counter-disinformation efforts into broader hybrid threat strategies.

In order to achieve its goals, NATO first expanded the role of its Strategic Communications Centre of Excellence (StratCom CoE), headquartered in Riga, Latvia. This centre plays a central role in monitoring disinformation trends, identifying emerging narratives, and developing counter-messaging strategies (Genini, 2025). The partnerships between the military and civilian units worked on intercepting hostile information campaigns and issuing rapid responses that framed NATO as not prepared enough or giving up on its Member States (Chłoń, 2022).

Secondly, the Alliance increased its investment in fact-checking and media literacy initiatives. Partnership with independent research institutions and think tanks allowed producing empirical studies on disinformation dissemination and contribute to education campaigns that would help the public counter misleading narratives. NATO also strengthened internal coordination by providing its communication teams in Brussels and other command structures with the latest intelligence on disinformation threats. This effort was expected to help retain clear, credible, and

anti-manipulation NATO's messaging thus recognising that the socio-cognitive dimension of hybrid threats where perception is a strategic contested aspect (Genini, 2025).

A third factor entailed direct cooperation with social media companies in order to counter disinformation online. Understanding that most of the misleading COVID-19 content was being shared over digital media platforms including Facebook, Twitter, and YouTube, NATO insisted on greater platforms' accountability. The Alliance worked with technological companies to flag state-backed propaganda, remove harmful content, and adjust algorithms to prevent the spread and limit the impact of false information (Tagliabue, Galassi, & Mariani, 2020). This collaboration helped limit the reach of certain disinformation campaigns, however it remained challenged by balancing content moderation while safeguarding freedom of speech.

Lastly, NATO incorporated counter-disinformation policies into broader hybrid threat strategies, meaning that COVID-19 disinformation responses became a method that was compatible with its overall security framework. The pandemic revealed that information warfare is not inseparable but a part of contemporary warfare. NATO therefore revised its doctrines to ensure that countermeasures to disinformation were integrated during exercises, crisis response planning, and discussions regarding defence policies (Ferreira Caceres et al., 2022).

Despite these efforts, NATO has faced great challenges in countering disinformation efforts. One major obstacle was navigating through the diverse political complexities of its 31 Member States, each with their unique view on free speech, media regulation, and crisis communication. Even though NATO was able to provide strategic guidance, the implementation of counter-disinformation policies had to be applied by the national governments leading to responses inconsistency. Such fragmentation highlights a wider conflict between supranational coordination and national sovereignty in managing hybrid threats. Moreover, NATO had to ensure that its counter-disinformation initiatives did not inadvertently fuel perceptions of censorship or propaganda, particularly in societies where government trust was already fragile (Hadlington et al., 2020).

4.2.2 The EU's regulatory and normative approach

Looking at the disinformation initiatives pursued at the European level, a clear-cut division of labour becomes noticeable, with NATO focusing on security and strategic dimensions, and the

EU specialising in the regulation of digital platforms, debunking false information, and coordinating responses among its Member States. The EU's commitment to uphold democratic values, ensure transparency, and foster media resilience can be seen in its main activities.

One of the EU's most significant initiatives is the East StratCom Task Force, an entity based out of the European External Action Service (EEAS) and responsible for monitoring and debunking foreign disinformation campaigns. The EUvsDisinfo project, a key component of the task force, has put much emphasis on actively tracking and exposing disinformation related to the COVID-19 pandemic, particularly from Russian and Chinese sources (Tagliabue, Galassi, & Mariani, 2020). Through a publicly accessible database, EUvsDisinfo provides fact-checks, analysis reports, and media literacy materials that can help citizens and policymakers better navigate the information environment. This was complemented by the Joint Communication on Tackling COVID-19 Disinformation, published by the European Commission and the High Representative in June 2020, that directly referred to "foreign actors and certain third countries, in particular Russia and China", as the main actors spreading disinformation during the pandemic. High Representative Josep Borell warned that "disinformation can kill" and emphasised the EU's responsibility to hold malign actors accountable while strengthening the block's digital resilience (European Commission, 2020).

In addition to monitoring, the EU used its regulatory power to pressure social media companies to take greater responsibility in content moderation. A voluntary 2018 Code of Practice on Disinformation was subsequently updated in 2022 to include binding components and culminated in the Digital Services Act (DSA). All of these measures required companies such as Facebook, Twitter, and Google to enhance their efforts in curbing false narratives, particularly during the pandemic and progressively strengthened the EU's leverage. The 2022 Code required proactive engagement with technological firms, urging them to remove harmful COVID-19 misinformation and provide greater transparency on moderation processes (British Academy, 2021). The DSA further institutionalised them by requiring VLOPs to identify and address systemic risks, improve access to platform data for independent researchers, and ensure accountability for algorithmic amplification of harmful content (European Commission, 2022). This legislative progression reflects the EU's strategic deployment of regulatory sovereignty as a resilience mechanism to shape the digital information ecosystem and counter hybrid threats.

Lastly, as a way of promoting digital literacy, the EU carried out campaigns on public awareness during the pandemic. These efforts aimed at empowering citizens by giving them the skills to critically analyse online information, recognize disinformation tactics, and identify credible sources. The cooperation of the European Commission and national governments promoted educational initiatives that encouraged media literacy at schools and among vulnerable populations (Ferreira Caceres et al., 2022). Such initiatives reflect a long-term normative investment in societal resilience, which is an implicit goal of HTT. At the same time, the EU also improved its information-sharing capacity by cooperating with NATO through the NATO-EU Task Force on Hybrid Threats, which ensured exchange information between the two organisations and promoted effective distribution of intelligence on disinformation threats. By combining NATO's security-focused approach and the EU's regulatory and educational strategies, both organisations were able to create a broad response to challenge of information during the pandemic (Genini, 2025).

Despite NATO and the EU's proactive measures, a number of challenges have reduced the effectiveness of such initiatives. Malign actors have been finding ways to evolve their strategies, using new technologies such as deepfake videos and AI-generated content, to make false narratives more credible. This constant evolution makes the task of fast-checking and digital platforms more difficult to pace (Hadlington et al., 2020). Many of these claims circulating on social media have not been challenged even with increased monitoring and content moderation investments. As a result, the systemic vaccine scepticism and distrust in public health responses has been highly maintained, forcing NATO as well as the EU to take into consideration that their counter-disinformation efforts should not interfere with the democratic freedoms (Ferreira Caceres et al., 2022). While in authoritarian information flows are controlled with state-imposed censorship, open societies have media plurality as a fundamental right (Tagliabue, Galassi, & Mariani, 2020). Moreover, differences in political priorities, regulatory frameworks, and levels of digital literacy among Member States have created fragmented responses that further weakened the collective resilience (British Academy, 2021).

The COVID-19 pandemic was as a critical test of NATO and the EU's ability to combat disinformation as a hybrid threat. False information was used to undermine trust in society by malign actors, particularly Russia and China, to drive societal divisions and weaken transatlantic unity. Disinformation campaigns during the pandemic were thus not isolated incidents but,

instead, part of a broader pattern of hybrid warfare whose goal is to destabilize democratic societies. Even though both organisations implemented significant responses, the crisis demonstrated the importance of for long-term resilience strategies. In the future, effective intelligence-sharing and joint strategic planning will become essential in meeting the challenge of hybrid threats in an increasingly digital information environment. Besides, the international community should develop binding regulatory frameworks as an alternative to voluntary codes of conduct to ensure accountability in the digital sphere. In line with such actions, it is crucial to continue developing digital literacy programs at the national and international levels since they empower citizens to critically assess information and strengthen cognitive resilience.

Overall, the handling of the COVID-19 related disinformation by NATO and the EU can be considered a valuable case study about the contemporary hybrid threat governance in practice. The experience shows that security oriented and regulatory approaches can complement each other despite institutional and political complexity. Since the tactics of adversaries increasingly become more sophisticated and socially focused, the key problem is not only to neutralise malign influence but to build cohesive, democratic resistance from within. This discussion thus continues in the following section by analysing how following the pandemic the EU enhanced its role within hybrid threat environment in a more salient way and how strengthening reliance with NATO has enabled closer integration of transatlantic response to hybrid warfare in an increasingly competitive world.

4.3 Evaluation of joint response: strengths, weaknesses, and lessons learned

The institutional responses of NATO and the EU to the COVID-19-related disinformation points both significant progress in tackling hybrid threats and long-standing structural weaknesses to operate effectively within the cognitive domain.

On the one hand, the crisis intensified operational synergy. NATO, to take an example, deployed its Strategic Communications Centre of Excellence to counter false narratives, issue public rebuttals, and coordinate with Member States on crisis communication (Smith, 2019; NATO, 2020). Simultaneously, the EU mobilized the EEAS and the East StratCom Task Force to detect and report on cases of disinformation revealing real time updates, as well as discovering hostile actors and malign narratives (European Commission, 2020; Filipec, 2021). Collectively, these practices represent the transitional shift in how institutions approach the information domain as

a strategic frontier, encompassing both operational and strategic dimensions. These parallel responses support the increasing awareness of the cognitive domain as a legitimate area of strategic interest, reflecting the evolution of HTT in the direction of influence operations and societal resilience. Both organisations started regarding information integrity not as a communications problem but as the core of democratic resilience, institutional legitimacy, and social cohesion. Cooperation on the political level was also enhanced with the high-level statements, informal working groups, and rhetorical emphasis on complementarity rather than competition (Anagnostakis, 2025; Uziębło, 2017).

Where NATO took its strong strategic communications infrastructure and military foresight capabilities, the EU took a set of regulatory regimes and civilian engagement mechanisms. Through its post-2016 DSA framework and its diplomatic actions, the EU enforced tools to target Russian media outlets with financial sanctions. Such division of labour, between NATO's security-centric approach and the EU's regulatory-technocratic focus, has provided an example of functional complementarities between the two organisations even where interoperability remained limited (Missiroli & Rühle, 2020; Van Raemdonck & Meyer, 2024). This strategic logic of interdependence as presented by RDT, rather than being based on hierarchical control, the institutions maintain cooperation through employing the strategic exchange of distinct capabilities which can be used to offset mutual vulnerabilities.

EU-NATO progress reports between 2017 and 2023 record this operational cooperation between NATO and the EU in countering hybrid threats, some of which are interdependence, documenting the operational, including disinformation and cyber operations. The table below gives a comparative analysis of their abilities to deal with such threats and shows the operational, normative, and structural assets each institution brings to the hybrid threat environment, underscoring the interdependence that guides their cooperation (EU-NATO, 2017-2023).

Table 3: NATO and EU capabilities in countering Disinformation

Capability	NATO	EU
Mandate type	Security, military, defence	Civilian, regulatory, normative
Tools	StratCom CoE, exercises, guidance	DSA, Code of Practice, EEAS, EDMO
Strengths	Intelligence, deterrence, foresight	Regulation, digital governance, media literacy
Limitations	No regulatory / legal mandate	No hard power, limited enforcement capacity
Role in COVID-19	Strategic communication, resilience narrative	Platform regulation, disinformation tracking

Source: Author's own elaboration

Even though every institution has different features, complementarity and comparative gaps influence the form of their collaboration. The mandate of both organisations, the resource availability, and the inadequacy of the coordination frameworks are narrow. The civilian mandate of NATO does not encompass controls on health, education, and digital platform regulation, where disinformation based on COVID-19 flourished. At the same time, the EU's regulatory tools such as the Code of Practice on Disinformation or the early drafts of the Digital Services Act, were either voluntary, slow-moving, or lacked consistent enforcement mechanisms (Milo, 2021; Jacuch, 2021). Such inertia created strategic blind spots, particularly in the early stages of the pandemic when disinformation was spreading widely and inter-institutional coordination was still in its early stages. These vulnerabilities were intentionally exploited by authoritarian actors to take advantage of the lack of a comprehensive, coordinated response.

Deeper collaboration was also hampered by institutional constraints. Although the rhetorical promotion of coordination by NATO and the EU, the operational interoperability of the information environment remained underdeveloped. Intelligence sharing was inconsistent, joint task forces were absent, and strategic narratives were not always harmonized across platforms and Member States. According to Missiroli and Rühle (2020), the notions of "total defence" and "societal resilience" were conceptualised differently by the two organisations. These differences show deeper divergences in political culture, institutional mandates, and strategic communication doctrines that limit the depth and effectiveness of joint responses. Through the lens of RDT, institutional autonomy and resource asymmetries such as disparities in personnel, funding, and legal mandates may limit collaboration and thereby the efficacies of joint actions. These difficulties also highlight divergent strategic cultures: NATO's deterrence logic that

emphasizes credible defence and command structure coordination, while the EU values soft-power governance and democratic norm-setting especially in the digital domain (De Maio, 2020; Pamment, 2020).

Nevertheless, the crisis left behind some critical lessons and outlined tangible opportunities of potential cooperation in the future. First, in the case of both NATO and the EU, there was an understanding that a more reactive approach must be shifted towards more anticipatory and preventive information strategies. Such a change not only encompasses such the early-warning mechanisms as detection and deterrence, but also offensive strategies aimed at pre-empting disinformation before it spreads (De Maio, 2020). Second, the crisis confirmed that hybrid threats require a “whole-of-society” response that mobilises institutions, civil society, media actors, and local communities in a collective effort to establish cognitive resilience. An immediate opportunity is institutionalizing joint situational awareness mechanisms. Although ad hoc cooperation is already possible through the Joint Task Force on Hybrid Threats and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE, 2017) in Helsinki, the absence of a permanent institutional framework limits long-term planning, rapid operational response, and sustained institutional memory (Szymański, 2020; Wiseman, 2021). The Hybrid CoE is now a central hub of training, analysis, and collaboration offering an essential space where NATO and the EU exchange expertise and best practices on methods of addressing hybrid threats, especially in the areas of disinformation and cyber warfare (Hybrid CoE, 2023).

A Joint Centre for Hybrid Threat Monitoring and Analysis, expanding the mandate of the existing Hybrid CoE, would centralize data collection, analysis, and dissemination of disinformation-related intelligence while also facilitating shared threat assessments, improving inter-institutional trust, and fostering coordination. The Joint Declaration of EU–NATO Cooperation in 2023, in turn, is a major step forward in this direction, further reinforcing the commitment to institutionalise these actions. Since it emphasises improved interoperability in hybrid threat response, the declaration offers both institutions a clear mandate to enhance cooperation, especially in joint situational awareness. It represents a shift towards permanent frameworks for intelligence-sharing and real-time threat analysis that aims to strengthen collaboration within NATO and the EU through the Hybrid CoE and the existing mechanisms (NATO, 2023).

Another opportunity is the creation of strong intelligence-sharing protocols that reduce the gap between military and civilian domains. With disinformation operations becoming progressively sophisticated using algorithmic amplification, artificial intelligence, deepfakes, and precision-targeted psychological operations, timely and secure information exchange is essential (Berzina et al., 2019). The advantages of NATO in terms of rapid threat identification and military intelligence can be coupled with the EU's regulatory oversight, civilian data access, and experience in public-sector communications. Current technical platforms, like the EU's FIMI Toolbox and NATO's Cognitive Warfare Initiative offer a solid foundation to this effort, as they serve as technical bridges, help foster a shared operational taxonomy and improve strategic integration between institutions (EEAS, 2023).

Equally important is the need to harmonize the strategic communication strategies. NATO's operational experience in military messaging, information operations, and counterpropaganda can complement the EU's legal-regulatory authority in the digital sphere, with the Digital Services Act and the Code of Practice on Disinformation serving as an illustration (European Commission, 2020; Pamment, 2020). A harmonized transatlantic approach to counter narratives, which encompasses both institutions' competencies, would allow the application of a dual-front strategy that targets both malign content as well as the digital ecosystems through which it proliferates. Institutionalizing the practice of joint simulation and crisis communication playbooks is a method of stress-testing and capacity-building across both civilian and military lines. Yet countering disinformation should go beyond institutional coordination to include building societal resilience that empowers citizens to resist manipulation by developing media literacy, civic education, and trust. Disinformation thrives in information environments where trust in institutions is low and critical thinking is lacking (Giussani, 2020). NATO and the EU are specifically aligned to work together on digital literacy campaigns that fill the gap between national education policies and transnational threats. By building on the grassroots initiatives of NATO, through the military families, veterans, youth programs, and realigning them with the EU work through contact with civil society organizations, schools, and municipalities, a more inclusive model of societal resilience can be ensured.

These cross-level efforts have the potential to bring together institutional actors with communities in a local setting. The suggested initiatives involve digital literacy curricula within schools, following the example of Finland, where the national integrated media literacy program

is largely coordinated by the state and lauded to instil critical thinking skills and resilience against misinformation in students, disinformation awareness workshops are designed to engage diverse community groups, and multilingual online toolkits are aimed to assist vulnerable populations in both urban and rural areas (European Commission, 2020; Pamment, 2020). Such measures are valuable not only to increase the levels of individual critical media consumption but also to encourage community-level vigilance, which causes societal resilience by establishing inclusive and context-sensitive education. Integrating it into the broader public policy frameworks will ensure that the effects of such programs last and correlate with the strategic objectives of both NATO and the EU to develop informed, resistant populations that can fight hybrid threats. In addition to public education, local capacity building is key. Multilateral training programs among journalists, municipal leaders, and community leaders can also be force multipliers that build networks of local resilience that are capable of preventing and responding to disinformation in real time. To ensure long-term sustainability, sufficient funding, public-private partnerships, and institutional recognition are essential.

Alongside these internal processes, NATO and the EU must move forward to develop their strategic cooperation to the multilateral normative arena. Transatlantic coordinated diplomacy in multilateral forums such as the UN, the OSCE, and the G7, can strengthen democratic standards and promote responsible state behaviour in the information domain (Berzina et al., 2019). When the EU's diplomatic reach and legal expertise is combined with NATO's security credibility and strategic convening power, there is a unified front. The joint initiatives can be negotiations of multilateral codes of conduct on foreign information operations, frameworks for attribution and verification, and an international observatory to monitor malign information campaigning. These efforts could not only reinforce global norms but also build a common transatlantic outlook on information and democratic resilience.

Despite these potential efforts, structural silos and divergent institutional logics are also a barrier to complete cooperation. Although NATO and the EU's capacities clearly demonstrate complementarity, they remain underleveraged. The COVID-19 pandemic demonstrated the strategic necessity and the operational difficulties of transatlantic cooperation in countering disinformation, highlighting the institutional vulnerabilities and at the same time demonstrating the effectiveness of coordinated action. NATO and the EU have shown that their own strengths, which are military strategy and regulatory capacity, can complement each other. Formalising,

scaling and institutionalising this cooperation is the next step. To achieve that, an interoperable infrastructure, shared doctrine, and a cohesive strategic culture is needed. Therefore, the transatlantic community should be able to meet these challenges with coherence, resilience, and foresight as adversaries continue to weaponise information in their attempts to destabilise democratic societies.

Conclusions and critical reflection

This thesis examines the dynamics of hybrid threats in the context of disinformation, focusing on the transatlantic cooperation between the North Atlantic Treaty (NATO) and the European Union (EU) during the COVID-19 pandemic. Based on the Hybrid Threat Theory (HTT) and Resource Dependence Theory (RDT), the paper evaluates the conceptualisation and modes of operation of disinformation by both institutions individually and jointly.

The findings reveal that the pandemic served as a factor of institutional adaptation. NATO deployed its military-strategic communication and rapid threat assessment capabilities, and the EU leveraged its normative power, creating regulatory frameworks such as the Digital Services Act (DSA) and the Code of Practice on Disinformation. Such a division of labour indicates that HTT was more concerned with multi-domain coordination and RDT emphasizes asymmetric dependence of resources as an incentive to inter-institutional cooperation (Biermann, 2014; Giegerich, 2016).

There are, however, some obstacles that limit the power of full integrated action. The presence of structural and operational limitations such as stovepipes in information-sharing, regulatory asymmetries, and divergent strategic cultures are evident (Zandee et al., 2021). The mandate makes NATO focus more on collective defence, restricting its role in normative areas such as platform accountability or digital rights. On the other hand, the EU struggles with institutional fragmentation and the slowness of regulatory implementation. RDT reveals that these issues are the results of disparities in institutional roles, resources, and external legitimacy. Thus, these challenges continue to weaken timely joint action, and it is clear that overcoming them will require legal harmonisation, trust-building, and increased cooperation with civil society (Filipec, 2023).

Despite these shortcomings, the pandemic strengthened the awareness of the information domain as a critical arena of strategic competition. New initiatives, including the Hybrid Centre of Excellence (Hyrid CoE) and exploratory proposals for joint situational awareness mechanisms, are indicators of the growing commitment to institutionalise hybrid threat responses into protocol. Such development is a significant step in the institutionalisation of the battle against disinformation as component of a broader strategy to protect democratic resilience (Wiseman, 2022).

In a critical perspective, the study points out an existing paradox of complementarity among the EU and NATO, whilst they are not fully used due to entrenched bureaucratic silos and political sensitivities. These obstacles must be resolved through legal and procedural harmonisation, an endeavour that cannot be achieved without overcoming such entrenched barriers and through the process of trust-building and civil society engagement, which is essential in developing democratic resilience and in increasing confidence in these institutions (Biermann, 2014; Zandee et al., 2021). Furthermore, the normative dilemma of countering disinformation and yet safeguarding democratic freedoms is still unresolved and demands further additional research. The constant struggle between regulation and the preservation of freedom of expression makes it difficult to address foreign manipulation of public opinion. The task will only become more acute as political and technological environments change, especially generative AI and deepfakes rise. That is why any strategy countering disinformation should be based on democratic legitimacy and long-term public trust (Genini, 2025).

Further research can elaborate on these findings by focusing on transatlantic responses to hybrid threats beyond disinformation, for example cyber intrusions or energy coercion. Moreover, it is crucial to explore how private technological platforms influence institutional resilience as they are at the core of the information ecosystem. Comparative research, in the context of heterogeneous national and regional frameworks, can provide useful combination of perspectives in regard to the variable geometry of hybrid threat governance, similarly highlighting differences in the manner in which NATO and the EU Member States address such challenges. Lessons from best practices around resilience building in front line states like Estonia, Latvia and Finland, can also provide guidelines that can have wider applicability. In addition, a more active division of labour between NATO and the EU, focusing on disinformation operations to other areas involving hybrid threats can be further developed. This way, one would be able to look at how the current form of cooperation can be replicated and optimised in order to address the wider hybrid threats' issues.

In conclusion, the COVID-19 pandemic has demonstrated major gaps in NATO and the EU's capabilities of responding to the issue of disinformation, and at the same time it has provided opportunities to promote joint efforts and strategic convergence. This crisis further highlighted that safeguarding democracy in the 21st century is not only a question of conventional military

deterrence but also an efficient protection of the information environment. Since hybrid threats are still transforming alongside the increase of technological advances and shifting geopolitical dynamics, it is crucial to build a cohesive and anticipatory transatlantic strategy. With the struggle to maintain democratic resilience globally, NATO-EU collaboration can be viewed as a blueprint of a more integrated, norm-driven strategy of safeguarding the democratic institutions in an increasingly hostile information environment.

Bibliography

- Anagnostakis, D. (2025) “‘Taming the Storm’ of Hybridity: The EU-NATO Relationship on Countering Hybrid Threats – From Functional Overlap to Functional Cooperation’, *Defence Studies*, pp. 1–25. Doi: <https://doi.org/10.1080/14702436.2025.2464636>
- Arcos, R. (2020). EU and NATO confront Hybrid Threats in Centre of Excellence - Rubén Arcos | Inteligencia | Comunicación | Amenazas Híbridas. [online] *Jane’s Intelligence Review*. Available at: <https://rubenarcos.com/pubs/eu-and-nato-confront-hybrid-threats-in-centre-of-excellence>
- Arcos, R. and Smith, H. (2021). Digital Communication and Hybrid Threats. *Revista ICONO14 Revista científica de Comunicación y Tecnologías emergentes*, 19(1), pp.1–14. doi: <https://doi.org/10.7195/ri14.v19i1.1662>
- Berzina, K. et al. (2019). European Efforts to Counter Disinformation. [online] *European Policy Blueprint for Countering Authoritarian Interference*, German Marshall Fund of the United States, pp.41–49. doi: <https://doi.org/10.2307/resrep21251.8>.
- Biermann, R. (2014). NATO’s Troubled Relations with Partner Organizations: A Resource-Dependence Explanation. *New Security Challenges Series ((NSECH))*, pp.215–233. Doi: https://doi.org/10.1057/9781137330307_12
- Biermann, R. and Harsch, M. (2016). Resource Dependence Theory. In : Koops, J., Biermann, R. (eds) *Palgrave Handbook of Inter-Organizational Relations in World Politics*, [online] Palgrave Macmillan, London, pp.135–155. Doi: https://doi.org/10.1057/978-1-137-36039-7_6
- Caceres, M.M.F., Sosa, J.P., Lawrence, J.A., Sestacovschi, C., Tidd-Johnson, A., Rasool, M.H.U., Gadamidi, V.K., Ozair, S., Pandav, K., Cuevas-Lou, C., Parrish, M., Rodriguez, I. and Fernandez, J.P. (2022). The Impact of Misinformation on the COVID-19 Pandemic. *AIMS Public Health*, [online] 9(2), pp.262–277. doi: <https://doi.org/10.3934/publichealth.2022018>
- Chłoń, T. (2022). NATO and Countering Disinformation. [online] *Globsec*. Available at: <https://euagenda.eu/upload/publications/nato-and-counteracting-disinformation-ver1-spreads.pdf>

Citron, D. and Chesney, R. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, [online] 107(6), p.1753. Available at: https://scholarship.law.bu.edu/faculty_scholarship/640/

Colom Piella, G. (2022). NATO's Strategies for Responding to Hybrid Conflicts. [online] *Cidob.org*. Available at: <https://www.cidob.org/en/publications/natos-strategies-responding-hybrid-conflicts>

Cullen, P. (2021). A perspective on EU hybrid threat early warning efforts. *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, pp.46-57.

De Maio, G. (2021). Opportunities to Deepen NATO-EU Cooperation. [online] *Foreign Policy at Brookings*. Available at: <https://www.brookings.edu/articles/opportunities-to-deepen-nato-eu-cooperation/>.

Doyle, K. and Desta, T. (2020). An Analysis of Common Security and Defence Policy's (CSDP) Strategic Communication (StratCom). *Journal of Politics and Law*, 14(2), p.56. doi: <https://doi.org/10.5539/jpl.v14n2p56>.

EDMO (2023). Disinformation narratives during the 2023 elections in Europe – EDMO. [online] *edmo.eu*. Available at: <https://edmo.eu/publications/disinformation-narratives-during-the-2023-elections-in-europe/>

EDMO (2023). March 2023 marks the dawn of AI generated mass disinformation – EDMO. [online] *Edmo.eu*. Available at: <https://www.idmo.it/en/2023/04/19/ai-disinformation/>

European Commission (2016). EUR-Lex - 52016JC0018 - EN - EUR-Lex. [online] *Europa.eu*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018>.

European Commission (2020). Coronavirus: EU strengthens action to tackle disinformation. [online] *ec.europa.eu*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006

European Commission (2020). Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the

Regions. Tackling COVID-19 Disinformation - Getting the Facts Right. [online] EUR-Lex. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0008>.

European Commission (2022). Code of Practice on Disinformation | Shaping Europe's Digital Future. [online] digital-strategy.ec.europa.eu. Available at: <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.

European Commission (2022). The Digital Services Act. [online] European Commission. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

European Commisison (2022). European citizenship - Publications Office of the EU. [online] Publications Office of the EU. Available at: <https://op.europa.eu/en/publication-detail/-/publication/7363758b-bc10-11ed-8912-01aa75ed71a1/language-en>

European Commission (2023). Standard Eurobarometer 98 - Winter 2022-2023. [online] europa.eu. Available at: <https://europa.eu/eurobarometer/surveys/detail/2872>

European External Action Service, EEAS (2015). Food-for-thought paper 'Countering Hybrid Threats'. [online] Statewatch.org. Council of the European Union. Available at: <https://www.statewatch.org/media/documents/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf>

EU-NATO (2017). Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170619_170614-Joint-progress-report-EU-NATO-EN.pdf

EU-NATO (2018). Third 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. Available from: <https://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf>

EU-NATO (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. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

EU-NATO (2020). Fifth 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. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf

EU-NATO (2021). Sixth 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. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf

EU-NATO (2022). Seventh 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. Available from: <https://www.consilium.europa.eu/media/57184/eu-nato-progress-report.pdf>

EU-NATO (2023). Eighth 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. Available from: <https://www.consilium.europa.eu/media/65076/st10254-en23.pdf>

Freedman, L. (2017). The Future of War: A History. [online] Google Books. Available at: https://books.google.de/books/about/The_Future_of_War.html?id=2_otDwAAQBAJ&redir_esc=y

Giegerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict on JSTOR. Jstor.org, [online] Vol. 15(No. 2 (Spring 2016), p.pp. 65-72. doi: <https://doi.org/10.2307/26326440>

Giussani, A. (2020). Competing over truth: a Critical Analysis of EU Initiatives to Counter Disinformation (2015-2019) - IKEE / Aristotle University of Thessaloniki - Library. [online] Available at: <https://ikee.lib.auth.gr/record/318872/files/>.

Genini, D. (2025). Countering Hybrid Threats: How NATO must adapt (again) after the War in Ukraine. New Perspective, 33(2). Doi: <https://doi.org/10.1177/2336825x251322719>

Gugulashvili, M. (2023). Lessons of Democratic Resilience: the EU and NATO Approaches Against Disinformation and Propaganda. [online] Georgian Center for Strategy and Development (GCSD). Available at:

[https://www.csd.org.ge/storage/files/doc/Lessons%20of%20Democratic%20Resilience%20-%20the%20EU%20and%20NATO%20Approaches%20Against%20Disinformation%20and%20Propaganda%20\(1\).pdf](https://www.csd.org.ge/storage/files/doc/Lessons%20of%20Democratic%20Resilience%20-%20the%20EU%20and%20NATO%20Approaches%20Against%20Disinformation%20and%20Propaganda%20(1).pdf)

Hartmann, U (2017). The Evolution of Hybrid Threats, and Resilience as a Countermeasure. [online] Nato Defence College. Available at: <https://www.ndc.nato.int/news/news.php?icode=1083>

Hoffman, F.G. (2010). 'Hybrid Threats': Neither Omnipotent Nor Unbeatable. *Orbis*, 54(3), pp.441–455. doi: <https://doi.org/10.1016/j.orbis.2010.04.009>.

Hybrid CoE (2017). Establishment. [online] Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. Available at: <https://www.hybridcoe.fi/establishment/>

Hybrid CoE (2024). What is Hybrid CoE. [online] Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. Available at: <https://www.hybridcoe.fi/who-what-and-how/>

Ivančík, R. and Nečas, P. (2022). On disinformation as a hybrid threat spread through social networks. *Entrepreneurship and Sustainability Issues*, 10(1), pp.344–357. Doi: [https://doi.org/10.9770/jesi.2022.10.1\(18\)](https://doi.org/10.9770/jesi.2022.10.1(18)).

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso, V.M., Lebrun, M., Aho, A. and Giannopolous, G. (2023). *Hybrid Threats: A Comprehensive Resilience Ecosystem*. JRC Publications Repository, [online] (ISBN 978-92-76-53293-4). Doi: <https://doi.org/10.2760/37899>.

Krulak, G.C.C. (1999). *The Strategic Corporal: Leadership in the Three Block War*. [online] apps.dtic.mil. Available at: <https://apps.dtic.mil/sti/citations/ADA399413>.

Lazer, D.M.J. et al. (2018). The Science of Fake News. *Science*, [online] 359(6380), pp.1094–1096. Doi: <https://doi.org/10.1126/science.aao2998>

Lewandowsky, S., Ecker, U. K. H., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the 'post-truth' era 6(4), 353–369. [online] psycnet.apa.org. Available at: <https://psycnet.apa.org/record/2017-57700-001>

Mattis, J.N. and Hoffman, F. (2005). Future Warfare: The Rise of Hybrid Wars. [online] U.S. Naval Institute. Available at: <https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars>.

Milo, D. (2021). The Deadly Effects of Disinformation. [online] CEPA. Available at: <https://cepa.org/article/the-deadly-effects-of-disinformation/>.

Missiroli, A. and Rühle, M. (2021). The Pandemic and the Military: EU and NATO Between Resilience and Total Defence. European Foreign Affairs Review, [online] 26(2). Available at: <https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.2/EERR2021016>

NATO (2010). Strategic Concept 2010. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_82705.htm

NATO (2014). StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. [online] stratcomcoe.org. Available at: <https://stratcomcoe.org>

NATO (2016). Warsaw Summit Communiqué - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO (2019). London Declaration. NATO. [online] 3 Dec. Available at: https://www.nato.int/cps/en/natohq/official_texts_171584.htm

NATO (2020). Remarks by NATO Secretary General Jens Stoltenberg on launching #NATO2030 - Strengthening the Alliance in an increasingly competitive world. [online] NATO. Available at: https://www.nato.int/cps/fr/natohq/opinions_176197.htm

NATO (2021). Summary of the NATO Artificial Intelligence Strategy. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_187617.htm

NATO (2022a). Madrid Summit Declaration issued by NATO Heads of State and Government (2022). [online] NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_196951.htm

NATO (2022b). NATO 2022 Strategic Concept. [online]. NATO. Available at: <https://www.nato.int/strategic-concept/>

NATO (2023). Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. [online]. NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_210549.htm

NATO (2024). Countering Hybrid Threats. [online]. NATO. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en

NATO (2020). NATO's approach to countering disinformation. [online]. NATO. Available at: <https://www.nato.int/cps/en/natohq/177273.htm>.

Filipec, O. (2023). The Cooperation between EU and NATO in Response to Hybrid Threats: a Retrospective Analysis from the Institutionalist Perspective. *Slovenská Politologická Revue*, [online] 23(1), pp.27–55. Available at: <https://www.ceeol.com/search/article-detail?id=1246667>.

Pamment, J. (2020). Front Matter. [online] *The EU's Role in Fighting Disinformation: Carnegie Endowment for International Peace*. doi: <https://doi.org/10.2307/resrep25788.1>.

Parkes, R. and Fiott, D. (2019). Protecting Europe: The EU's response to hybrid threats. [online] *JSTOR, European Union Institute for Security Studies (EUISS)*, pp.4–10 Introduction. Available at : <https://www.jstor.org/stable/resrep21143.4>

Pawlak, P (2015). Understanding Hybrid Threats: Origins, challenges and Policy Responses. [online] *Policycommons.net*. Available at: <https://policycommons.net/artifacts/1336169/understanding-hybrid-threats/1943129/>

Pawlak, P. (2017). Countering Hybrid Threats: EU-NATO cooperation. [online] *Policycommons.net*. Available at: <https://policycommons.net/artifacts/1338529/countering-hybrid-threats/1947195/>

Pennycook, G. and Rand, D.G. (2019). Fighting Misinformation on Social Media Using Crowdsourced Judgments of News Source Quality. [online] *ResearchGate*. Available at:

<https://www.researchgate.net/publication/330710636> Fighting misinformation on social media using crowdsourced judgments of news source quality

Rühle, M. (2019). NATO's Response to Hybrid Threats. [online] <https://nipp.org>. Available at: https://nipp.org/information_series/ruhe-michael-natos-response-to-hybrid-threats-information-series-no-448/

Schmitt, M.N. (2024). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2nd Edition | Cambridge University Press & Assessment. [online] Cambridge University Press & Assessment. Available at: <https://www.cambridge.org/de/universitypress/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB>

Szymański, P. (2020). Towards Greater resilience: NATO and the EU on Hybrid Threats. [online] Ceeol.com. Available at: <https://www.ceeol.com/search/gray-literature-detail?id=1164303>.

Shao, C. et al. (2018). The Spread of low-credibility Content by Social Bots. Nature Communications, [online] 9(1). Doi: <https://doi.org/10.1038/s41467-018-06930-7>

Starbird, K. (2017). Examining the Alternative Media Ecosystem through the Production of Alternative Narratives of Mass Shooting Events on Twitter. [online] University of Washington, HCDE. Available at: https://faculty.washington.edu/kstarbi/Alt_Narratives_ICWSM17-CameraReady.pdf

Tagliabue, F., Galassi, L. and Mariani, P. (2020). The 'Pandemic' of Disinformation in COVID-19. SN Comprehensive Clinical Medicine, 2(1287-1289). doi: <https://doi.org/10.1007/s42399-020-00439-1>.

Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K. and McCue, M. (2018). Addressing Hybrid Threats. [online] DIVA. Available at: <https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1219292&dswid=-3174>

Uziębło, J.J (2017). United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats. EU Diplomacy Papers, 5(5).

Van Raemdonck, N., and Meyer, T. (2024). Chapter 4: Why disinformation is here to stay. A socio-technical analysis of disinformation as a hybrid threat. In *Addressing Hybrid Threats*, Cheltenham, UK: Edward Elgar Publishing. available from: <https://doi.org/10.4337/9781802207408.00009>

Vosoughi, S., Roy, D. and Aral, S. (2018). The Spread of True and False News Online. *Science*, [online] 359(6380), pp.1146–1151. Doi: <https://doi.org/10.1126/science.aap9559>

Wiseman, J. (2022). *EU-NATO Hybrid Warfare*. NATO Science for Peace and Security Series – D: Information and Communication Security. Doi: <https://doi.org/10.3233/nicsp220015>

Zandee, D., Van der Meer, S. and Stoetman, A. (2021). *Countering Hybrid Threats Steps for improving EU-NATO cooperation*. [online] www.clingendael.org. Available at: <https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/>