ELISA ORRÙ

How the notion of "hybrid threat" is reshaping security. The case of migration and disinformation within the EU and its implications for the rule of law and democracy

This article examines the emergence of the concept of "hybrid threats" in EU security policy, and its implications for fundamental principles of the rule of law and democracy. It discusses these dynamics by focusing on two exemplary phenomena that have been framed as "hybrid threats": migration and disinformation. The article's main argument is that characterising these phenomena as "hybrid threats" leads to an increased intertwining of civil and military, internal and external dimensions of security, resulting in a "hybridisation" of security policies. Ultimately, this shifts the emphasis of securitisation towards the extreme pole of "existential threats". This places significant pressure on the fundamental principles of the rule of law, such as respect for fundamental rights and judicial control over executive powers, and also undermines democratic participation and the integrity of public discourse.

Hybrid threats – Security Union – Area of Freedom, Security and Justice – Disinformation – Migration Securitisation

"Minacce ibride" e ridefinizione della sicurezza. Le misure Ue nel campo della migrazione e della disinformazione e le implicazioni per lo Stato di diritto e la democrazia

L'articolo esamina l'emergere del concetto di "minacce ibride" nelle politiche di sicurezza dell'Ue e le sue implicazioni per i principi fondamentali dello Stato di diritto e della democrazia. Il saggio analizza queste dinamiche concentrandosi su due esempi emblematici di fenomeni che sono stati progressivamente e sempre più decisamente caratterizzati come "minacce ibride": la migrazione e la disinformazione. L'argomento principale dell'articolo è che definire questi fenomeni "minacce ibride" determina una crescente interconnessione tra le dimensioni civile e militare, interna ed esterna della sicurezza, con conseguente "ibridazione" delle politiche di sicurezza. In ultima analisi, tale processo sposta l'accento delle misure di sicurezza verso il polo estremo della risposta a "minacce esistenziali". Ciò esercita una pressione significativa sui principi fondamentali dello Stato di diritto, quali il rispetto dei diritti fondamentali e il controllo giudiziario sui poteri esecutivi, e rischia di compromettere la partecipazione democratica e l'integrità del dibattito pubblico.

Minacce ibride – Unione della sicurezza – Spazio di libertà, sicurezza e giustizia – Disinformazione – Migrazione Securitizzazione

The Author is Senior Researcher at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg and at Freiburg University

SUMMARY: 1. Introduction. – 2. Three phases of European internal security: institutionalisation. – algorithmisation – hybridisation. – 3. The current process of hybridisation of European Security. – 3.1. Key concepts: Security Union, collective security and hybrid threats. – 3.2. Two exemplary hybrid threats: the "instrumentalisation of migration" and disinformation campaigns. – 3.3. The parallel processes of securitisation and hybridisation in the fields of migration and disinformation. – 4. Implications for the rule of law and democracy. – 5. Conclusion.

1. Introduction

This article[1] explores the current dynamics within the field of European common security politics, arguing that there is an ongoing strong tendency towards the progressive hybridisation of internal and civil security with military and external security. This process is driven by an increasing framing of phenomena such as cyberattacks, migration and disinformation as "hybrid threats".

The article analyses in particular recent measures taken at the EU level to deal with two prototypical phenomena framed as "hybrid threats", namely the so-called "instrumentalisation of migration" and disinformation campaigns. It observes that EU measures adopted in response to these phenomena have coalesced around two key actors: the European Border and Coast Guard Agency (EBCG), commonly known as Frontex, and the European External Action Service (EEAS). In both cases, there has been increased entanglement of the internal and civil security dimensions with the external and military dimensions. This is exemplified by Frontex's strengthened cooperation with military actors such as the North Atlantic Treaty Organisation (NATO) and the allocation of critical tasks to the EEAS, the agency responsible for the EU's common external policies.

The article further considers how this shift imposes significant strain on fundamental principles of the rule of law and democracy. On the one hand, pre-existing deficiencies such as the lack of parliamentary oversight and judicial control over Frontex's actions are exacerbated by the growing "exceptionalism" that stems from framing migration as a hybrid threat. On the other hand,

---

treating disinformation as an existential threat to be addressed using military methods and logic is contrary to the concept of a democratic public sphere, which, as Hannah Arendt points out, is nourished by the exchange of differing opinions rather than the pursuit of truth.

The article proceeds as follows. Section 2 provides an overview of the historical development of a common European internal security policy area, identifying three phases of institutionalisation, algorithmisation, and hybridisation. Section 3 focuses on the ongoing third phase (hybridisation) and explores the measures taken to counteract two exemplary phenomena framed as "hybrid threats": migration and disinformation. Section 4 discusses the implications of the hybridisation of EU security for the rule of law and democracy. Finally, Section 5 concludes by summarizing the article's main arguments.

2. Three phases of European internal security: institutionalisation – algorithmisation – hybridisation

The first nucleus of today's European Union (EU) — the European Coal and Steel Community (ECSC) — was established in the aftermath of the Second World War, driven by the motivation to place the raw materials essential for waging war under the control of the Community. This was intended to discourage European states from resorting to war against each other again. Since the very beginning of the European integration process, therefore, a connection to security has been present. However, attempts to create a common defence policy were quickly abandoned in favour of transferring defence and military cooperation competences to NATO[2]. Consequently, when the Treaty of Rome, which established the European Economic Community (EEC), was signed in 1957, it focused solely on economic integration and made no provision for security cooperation, either internal or external.

However, as early as the 1970s, EEC Member States had already begun informal cooperation in matters of security. From 1976 until 1993, the interior and justice ministers of each state met twice a year at TREVI (*Terrorisme, Radicalisme et Violence Internationale*) group meetings to discuss organised crime, terrorism, police cooperation and migration[3]. An important milestone in the formalisation of security cooperation in Europe was the signing of the Schengen treaties in 1985 and 1990. After the European Commission's proposal to abolish controls at European internal borders was rejected by some Member States, a smaller group of states decided to sign international treaties outside the European Community's framework, intending to act as a catalyst for accession by further states. As the abolition of border controls between the signatory states was perceived by relevant actors as reducing security, "compensatory" measures to strengthen police and judicial cooperation, as well as the first European database — the Schengen Information System (SIS) — were introduced[4].

This first phase of European security integration culminated in the 1992 Treaty of Maastricht and the 1997 Treaty of Amsterdam, which incorporated the previously informal or intergovernmental cooperation — including the Schengen acquis — into the institutional framework of the EU and formally established the "Area of Freedom, Security and Justice" (AFSJ) as an EU policy area.

During this initial phase of European security integration, internal security was primarily presented as a necessary measure to support the implementation of the common market, particularly the four freedoms of movement of goods, services, capital and people. Security cooperation among Member States was officially regarded primarily in terms of "flanking measures" to achieve market integration and address the challenges arising from it. There were also strategic reasons for this: as the core competences transferred to European institutions were of economic nature, the connection to the realisation of the common market was central to avoiding criticism of the ECC and later EU institutions for acting *ultra vires*.

The most significant feature of this initial phase was the progressive institutionalisation of security cooperation. Practices originating from informal cooperation, such as the TREVI meetings, or from cooperation occurring outside the institu-

---

2. Holzhacker–Luif 2014.

3. *Ibidem*; Monar 2001.

4. Peers 2017.

tional framework of the European Communities, such as that following the Schengen treaties, were gradually incorporated into the EU. The informal and intergovernmental origins of these practices continued to shape European security cooperation even after it was transferred to the EU institutional framework. Indeed, EU security policies have long been characterised by a clear primacy of executive powers over parliamentary deliberation and judicial control[5].

The second phase of European security cooperation began around the turn of the millennium. It was characterised by strategic programmes from the European Council, including the Tampere, Hague and Stockholm programmes, and culminated in 2015 with a critical communication from the EU Commission: the "European Agenda for Security" (hereafter referred to as the "Security Agenda")[6]. During this phase, common European security measures predominantly focused on information exchange. This was given precedence over operational cooperation since security politics were still considered a core sovereign competence of individual states. By contrast, information exchange could more easily be presented as merely facilitating coordination between national agencies, despite the fact that EU initiatives also played a significant role in intensifying national security measures in practice[7].

During the second phase, a series of large databases were established, equipped with increasingly sophisticated search and analysis functions. The previously existing SIS was progressively equipped with new functionalities and flanked by the biometric database Eurodac, the Visa Information System (VIS) and, more recently, the decentralised Passenger Name Record (PNR) system. Other systems that have been established include the

Entry/Exit System (EES) and European Travel Information and Authorisation System (ETIAS), expected to become operational in 2025 and 2026 respectively. During this phase, alphanumerical systems such as SIS were equipped with biometric functions and new search functionalities. Binary verification logics were complemented with risk assessment functions and interoperability between the different systems became imperative.

This second phase continued until around 2020, marking both continuity and rupture with the first phase. On the one hand, the official focus continued to be on internal or civil security measures, as opposed to external or military security measures, although a tendency to blur this distinction was starting to emerge, particularly with regard to border controls[8]. On the other hand, this second phase departed from the narrative of the first phase, according to which security cooperation within the EU was functional to maintaining the free internal market. In contrast, in this second phase, relevant national and European actors increasingly viewed enforcing security within the EU as an end in itself that did not need to be justified by its contribution to the realisation of the internal market. This meant that security could be enforced, if necessary, even at the expense of the previously prioritised freedoms of movement[9].

In addition to continuing the trend of supra-nationalisation that began in the first emergent phase of EU security policy, the second phase was characterised by what has been termed the "algorithmisation of security"[10]. The aforementioned expansion of the EU's large database and of information exchange was not merely a quantitative increment. Rather, it has brought about a qualitative shift from norm-based, reactive verification systems used to identify individuals already known

---

5.   de Waele 2017; Holzhacker–Luif 2014.

6.   European Commission, *The European Agenda on Security,* COM(2015) 185; European Council *The Stockholm Programme - An open and secure Europe serving and protecting the citizens*, 2 December 2009; European Council, *The Hague Programme: strengthening freedom, security and justice in the European Union*, 2005/C 53/01; European Council, *Tampere European Council 15 and 16 October 1999. Presidency Conclusions*, 1999.

7.   Orrù 2022-b, 172; Orrù 2021, p. 141.

8.   Poscher 2016, p. 68; Bigo 2000, p. 171, pp. 186-188.

9.   Orrù 2022-b, pp. 204-206; Orrù 2021, pp. 277-283; Bellanova–de Goede 2020. Specifically on the relationship between the values of security, freedom and justice see Orrù 2022-a.

10. Bellanova–de Goede 2020. See also literature on algorithmic regulation, on which the concept of algorithmic security builds: Ulbricht 2018; Yeung 2018.

to the authorities, to investigative, risk-based, and pre-emptive tools used to identify potential "suspect" individuals who are not yet known to the authorities[11]. This new security logic, which is especially evident in the risk-based approach of the EU PNR directive and the upcoming ETIAS, aims to produce a probabilistic assessment of people's future behaviour. Under this approach, individuals are no longer evaluated based on their adherence to or violation of pre-established, relatively stable and widely recognised rules. Instead, they are profiled and sorted into risk categories based on "mobile", data-driven and opaque norms[12].

This risk-based, data-driven, pre-emptive approach to security challenges fundamental principles of the rule of law[13] and threatens to undermine anti-discrimination safeguards[14]. Moreover, it is based on an altered relationship between facts and norms, which has significant consequences for how legal and political issues are addressed by the law. At the heart of legal systems based on the rule of law is the "normative force" of the law. This lies in regulation that explicitly and transparently connects legal facts with legal consequences, providing a clear reference for legal subjects to orient their behaviour[15]. Data-driven, risk-based, pre-emptive security departs from this model as it explicitly renounces providing legal subjects with clear, stable, and intelligible norms of conduct. This deprives them not only of effective redress mechanisms[16], but also redefines the relationship between the legal and political systems and their subjects in a way that discards human autonomy. Rather than being seen as moral agents who can orient their conduct based on general and intelligible norms, subjects are now viewed as trait carriers to be profiled, rated, predicted and, if deemed appropriate, stopped[17].

Finally, while the main tendencies of the first two phases — namely, supranationalisation and algorithmisation — were still unfolding, a third tendency began to emerge. I suggest referring to this tendency as "hybridisation", as it involves an increasing connection between civil and military, internal and external security. By around the year 2020, this tendency had become the dominant feature of current developments within European security measures. The central drivers of this process are phenomena categorised as hybrid threats, such as cyberattacks, the so-called "instrumentalisation of migration" at European borders, and disinformation campaigns. As these threats blur the traditional line between the military and civil domains — so the main argument justifying this development in European security — they require an equally "hybrid" response. This third phase, its key concepts, dynamics, and challenges are the subject of the following sections.

3. The current process of hybridisation of European Security

As mentioned above, the convergence of internal and external security dimensions is not a new phenomenon, nor did it emerge abruptly. This trend has been observed by scholars since the beginning of the new millennium[18] and, as we will shortly see, has intensified since 2016. However, it seems reasonable to suggest that, since around 2020, this trend has been the driving force behind the most significant current developments in the field of EU security.

3.1. Key concepts: Security Union, collective security and hybrid threats

The strengthening of this tendency is reflected in EU strategic documents through the emergence of three key concepts: "Security Union", "collective

---

11. For a detailed analysis of this process, see Orrù 2022-b; Orrù 2021; Mitsilegas 2020; Mitsilegas 2015.

12. Leese 2014, p. 505; Amoore 2011, p. 31.

13. Bayamlioğlu–Leenes 2018; Hildebrandt 2018; Yeung 2018; Hildebrandt 2016.

14. Leese 2014. For the discriminatory potential of Big Data probabilistic models in general see O'Neil 2016.

15. Bayamlioğlu–Leenes 2018, p. 305. See also Raz 1977.

16. Bayamlioğlu–Leenes 2018, p. 309.

17. In more detail Orrù 2022-c. For a broader reflection on human agency and algorithmic "rule" see Frischmann–Selinger 2018; Hildebrandt–Rouvroy 2011.

18. See footnote 8 above.

security" and "hybrid threats". "Security Union" refers to the EU's responsibility to guarantee a high level of security throughout its Member States' territory. This term is not mentioned in EU primary law, but first appeared in an EU official document in the form of a communication issued by the European Commission (EC) in 2016, containing guidelines for implementing the 2015 Security Agenda[19]. As noted above, the latter document marked the culmination of the second phase of European security policy. Despite its being formally a mere "specification" of the previous document, the 2016 Commission's Communication actually initiated a transformation process. Although "AFSJ" is still the official term — and the one set out in EU primary law — to define the policy area of cooperation in security matters, it has been completely replaced by the 2016 newly introduced expression "Security Union" in EU strategic documents over time. A 2020 EC Communication on the EU Security Union Strategy (hereafter referred to as the "Security Union Strategy") is emblematic of this substitution process. This document only uses the expression "Security Union" and never mentions the AFSJ, thus formally reflecting the prioritisation of security over the values of freedom and justice that the term "AFSJ" encompassed[20].

A key idea behind the concept of a "Security Union" is the need to move away from a purely cooperative approach and towards one that aims to protect "the collective security of the Union as a whole"[21]. Conceptualising the EU as a collective security space and actor marks a departure from intergovernmental approaches. According to this new framing, security in the EU requires centralised powers for EU institutions and agencies, rather than being a matter for the cooperation of its Member States[22]. This represents a significant shift for a policy area that has traditionally formed the core of state sovereignty. This shift is all the more significant when considered alongside the call for convergence of internal and external, civil and military security. Indeed, the 2020 Security Union Strategy encourages EU institutions to cooperate closely with military organisations, including NATO, and adopt a "whole-of-society approach"[23], connecting the civil, military and political spheres closely with each other[24].

The keystone of this reframing of EU security and the core justification for its collectivisation is the concept of "hybrid threats". A hybrid threat, according to the European Commission's definition, consists of a "mixture of coercive and subversive activity, conventional and unconventional methods […], which can be used in a coordinate manner by state or non-state actors"[25]. By definition, hybrid threats blur the distinction between the internal and external, civil and military spheres. It is this indistinctness that provides the justification for "hybrid" responses: in order to effectively counteract hybrid threats, the argument goes, responses must be able to draw on and connect resources from both the internal and external, civil and military domains.

---

19. The expression "Security Union" was actually used once before 2016 in official ECC/EU documents, namely in the minutes of a 1991 European Parliament sitting (European Parliament, *Minutes of the Sitting of Monday, 10 June 1991*, Official Journal of the European Communities, vol. 34, 1991, p. 23). Against the backdrop of the First Gulf War, the text calls for the arms sector to become part of the common European market within the context of a "Security Union". Therefore, the expression had a different meaning in 1991 than it did in 2016. While the former referred to the "communitarisation" of armaments production, the latter designated the objective of a stronger EU policy in the field of internal and civil security.

20. European Commission, *The EU Security Union Strategy*, COM(2020) 605.

21. European Commission, *Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union,* COM(2016) 230, p. 2.

22. On the EU as a collective security actor see KAUNERT–LÉONARD 2023; LUCARELLI–SPERLING–WEBBER 2020; SPERLING–WEBBER 2017.

23. European Commission, *The EU Security Union Strategy*, COM(2020) 605, p. 2.

24. GIANNOPOULOS–SMITH–THEOCHARIDOU 2021, p. 2.

25. European Commission, *The EU Security Union Strategy*, COM(2020) 605, p. 1; European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Framework on Countering Hybrid Threats. A European Union Response*, JOIN(2016) 18, p. 2.

The following recent statement from the President of the European Commission exemplary summarises the interplay of these concepts and their mutual reinforcement in current EU politics:

> Extraordinary times call for extraordinary measures. […] To deal with the challenging way ahead, we need to switch into a preparedness mind-set. […] From *external and internal security* to energy, defence and research. From cyber, to trade, to foreign interference. Only if we have a clear and in-depth understanding of the threats, including *hybrid threats*, can we effectively contribute to *collective security*[26].

3.2. Two exemplary hybrid threats: the "instrumentalisation of migration" and disinformation campaigns

In recent strategic documents, the EC has fleshed out the notion of hybrid threats in more detail. These include, for example, the "instrumentalisation of migrants" at the EU's external borders, the misuse of artificial intelligence for cyberattacks and information manipulation, and attacks on critical infrastructure[27]. The Council of the EU has also concerned itself with hybrid threats, launching the EU Hybrid Toolbox and a plan to establish Hybrid Rapid Response Teams in 2022. The Toolbox is intended to facilitate coordinated responses to hybrid threats, potentially involving "the full mobilisation of all relevant civilian and military instruments where appropriate, drawing from external and internal policies"[28], whereas the Hybrid Rapid Response Teams are designed to support and coordinate efforts among Member States.

Beyond establishing these overarching, albeit still quite generic, measures, a series of actions have been taken at EU level to address specific "hybrid threats". The following focuses on two paradigmatic phenomena that have been categorised as hybrid threats, triggering different institutional dynamics within the EU: the "instrumentalisation of migration" and disinformation campaigns. The former has been used to describe the strategic opening of Turkey's and Belarus' borders to the EU in 2020 and 2021, respectively. This has given new impetus to the long-term securitisation of migration[29] within the EU and the expansion and strengthening of the EU's primary migration policy actor, Frontex. By contrast, reactions to disinformation campaigns have so far resulted in relatively fragmented actions that have not yet been translated into the operational strengthening of institutions and agencies comparable to that concerning Frontex. However, as we will see below, there is a clear convergence between the civil and military domains in this field as well, particularly with regard to the competencies of another EU agency: the EEAS.

Beginning with the first phenomenon, framing migration as a "hybrid threat" has intensified existing dynamics that have long characterised Frontex's development. Established in 2004 by Council Regulation[30], the EU Agency since its early days exhibited some military-like structures, such as the Frontex Situation Centre, a real-time monitoring centre operational since 2009[31]. Furthermore, from the time of its creation, Frontex has been one of the EU agencies that has grown most rapidly and massively, expanding significantly in terms of equipment, budget and personnel. Initially presenting itself as a mere facilitator of cooperation between Member States[32], Frontex

---

26. Speech by Ursula von den Leyen of 9 March 2025, as quoted in Sason–Monti–Olivares-Martinez 2025, emphasis added.

27. European Commission, *ProtectEU: a European Internal Security Strategy*, COM(2025) 148, p. 11; European Commission, *Seventh Progress Report on the implementation of the EU Security Union Strategy*, COM(2024) 198, p. 1.

28. Council of the EU, *A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security*, 21 March 2022, p. 22.

29. den Boer 2008; Bigo 2002.

30. Regulation (EC) No 2007/2004 of 26 October 2004 *establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union* (no longer in force).

31. Léonard 2010, p. 243.

32. Ellebrecht 2020, p. 145.

has evolved into an agency with a high degree of autonomy in relation to EU institutions, acting as a controller of Member States' capacity to enforce border control[33]. The "migration crises" of 2005–2006 and 2015–2016 were crucial in facilitating this rise. Since 2016, the tendency towards militarisation has been explicitly sustained through the formalisation of cooperation between Frontex and NATO[34].

The framing of Turkey's and Belarus' respective strategic opening of their borders to the EU in 2020 and 2021 as "hybrid threats" intersected with and further boosted this process of militarisation. Indeed, between 2021 and 2022, Frontex's Rapid Border Intervention Teams (RABITs) contributed to the militarisation of the Turkish and Belarusian borders with the EU by deploying border guards and technical tools to support operations. Following Russia's invasion of Ukraine in 2022, moreover, Frontex participated in rapid response and surveillance operations on the Ukrainian border, taking on responsibilities akin to those of a military operation[35].

These developments have led the EU migration policies to move towards the extreme pole of the securitisation continuum, characterised by "survival, existential threat, and militarisation"[36]. Combined with other unique Frontex features, such as units with direct operational capabilities (the aforementioned RABITs) and staff directly employed by the agency (rather than Member States), this makes Frontex probably the EU agency with the highest level of supranationalisation of operational capabilities. Furthermore, beyond its operational capacities at European borders, Frontex is responsible for running the border surveillance system EUROSUR and, once operational, the ETIAS database.

The second prototypical "hybrid threat", disinformation, has been tackled by EU institutions in various, and partly contradictory, ways. Firstly, the EU has recommended actions aimed at fostering transparency and pluralism in the media, as well as promoting media literacy[37]. Secondly, a co-regulation approach has been adopted, culminating in the Digital Services Act. This obliges the leading digital platforms to counter and remove "illegal content", thereby imposing duties on private commercial actors to counter disinformation. Thirdly, the EU has adopted a securitisation approach, resulting in EU actions converging around the EEAS (the EU agency coordinating the common foreign and security policy)[38]. Since 2015, the EEAS has been responsible for addressing "Foreign Information Manipulation and Interference" (FIMI), with a particular focus on Russian disinformation. Several subgroups have been set up within the EEAS to tackle disinformation, including the "East StratCom" team and the EU Hybrid Fusion Cell[39].

The names of these committees and groups clearly reflect a geopolitical security terminology and thinking. The choice of the EEAS as the main actor entrusted with countering disinformation is symptomatic of the securitisation and hybridisation processes occurring[40]. Indeed, the EEAS is the nucleus of the still embryonic military cooperation within the EU, running the few existing joint military operations at the EU level. These include the European Union Naval Force (EUNAVFOR) Operation Atalanta in the Horn of Africa and the Western Indian Ocean, as well as the EUNAVFOR Aspides Operation in the Red Sea and the Gulf of Aden, which were initiated in 2008 and 2024, respectively. It is not obvious why the EEAS was chosen as the main actor to deal with disinformation: even within the common security policy area, other EU institutions within DG Home or DG

---

33. Sarantaki 2023, pp. 28-34.

34. Léonard–Kaunert 2022, p. 1425.

35. Sarantaki 2023, pp. 163-166.

36. Léonard–Kaunert 2022, 1417.

37. European Commission 2018.

38. Casero-Ripollés–Tuñón–Bouza-García 2023.

39. See European External Action Service, *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*.

40. Casero-Ripollés–Tuñón–Bouza-García 2023, p. 7.

Justice, for instance, could have provided closer links to EU actors who have long experience of dealing with disinformation, such as journalists, fact-checkers and media activists[41].

The EU's approach to disinformation has thus been characterised by a twofold process of securitisation. It has first been framed as a security issue, and secondly, within the securitisation spectrum and specifically through its classification as a hybrid threat, it has been allocated to the domain of external and military security. In this context, it is important to note that disinformation emerged in Europe as a politically preeminent issue ahead of the 2019 European elections and again during the 2020-21 COVID-19 pandemic. In both cases, as reflected in the High-Level Group's 2018 report on fake news and disinformation online, disinformation was not primarily considered a security issue. Indeed, the Group's 2018 report emphasises the need for measures to enhance the transparency of online news, promote media literacy, support users and journalists, and protect media pluralism — all of which have very little connection to security policy[42].

3.3. The parallel processes of securitisation and hybridisation in the fields of migration and disinformation

We can now draw an interim conclusion from the above analysis of the two prototypical hybrid threat phenomena. In both cases, two tendencies have subsequently developed in each field, running in parallel.

Firstly, the relevant phenomena have been categorised as a security issue. This is the classic securitising process that has long been observed and analysed in the field of migration, but has only recently emerged in connection with disinformation[43]. For both phenomena, this framing in terms of security issues is the result of actions taken by relevant political actors, rather than being something inherent to the phenomena themselves. During

the post-Second World War economic growth in some European countries, for example, human mobility and immigration were mostly considered in economic terms, as a needed workforce to sustain the growing economy. As we have just seen, similarly, disinformation was initially considered a matter potentially affecting democratic processes and public health policies. Securitisation processes have progressively strained these earlier understandings. For example, migrants have increasingly been depicted as "criminals", resulting in a series of connected discourses and policies that have shaped several European states' approaches to migration for decades. In the case of disinformation, the initial securitisation has occurred more recently and at a less visible level, for example through legislation that criminalises the spread of disinformation within national states[44].

The second tendency, which has stepped in on top of, or in connection with, the first securitisation step, is specifically brought about by framing the phenomena as "hybrid threats". This second step moves issues along the securitisation spectrum towards militarisation and has prompted the current process of hybridisation of security within EU policy, namely the convergence of civil and military, internal and external security. While the two steps are clearly separated in the case of migration, with an initial long period of securitisation followed more recently by a "hybridisation" phase, in the case of disinformation the two processes occurred almost simultaneously. In both cases, this second step has involved closer interlinking of internal and external, civil and military domains in EU policy – in short, a "hybridisation" of EU security.

4. Implications for the rule of law and democracy

Overall, the above developments, which integrate an ongoing securitisation process with the hybridisation of internal and external security, put

---

41. *Ivi*, p. 6.

42. European Commission 2018.

43. On securitisation in general, see Buzan–Wæver 2003, p. 71. On the securitisation of migration see exemplarily Léonard–Kaunert 2022; den Boer 2008; Bigo 2002. On the securitisation of disinformation Casero-Ripollés–Tuñón–Bouza-García 2023.

44. For an overview of newly introduced criminal provisions against disinformation and related acts such as deep-fakes in EU States see Bleyer-Simon–Horowitz–Botan et al. 2025.

ELISA ORRÙ

How the notion of "hybrid threat" is reshaping security. The case of migration and disinformation within the EU …

considerable pressure on the rule of law and basic democratic principles. Securitisation itself tends towards exceptionalism, namely the lowering of power-restricting mechanisms under the guise of a state of emergency. The process of hybridisation adds further intensity to this trend. The opening of von der Leyen's aforementioned speech ("Extraordinary times call for extraordinary measures") is a particularly effective example of this justification strategy.

The dynamics at work within the two fields of action addressing the two prototypical hybrid threats illustrate the mechanisms at play. Both Frontex and the European External Action Service are decentralised EU agencies which, by virtue of this, already enjoy a great margin of autonomy from EU institutional control. Within Frontex's Management Board, for example, the Commission has only two representatives who can easily be outvoted by the national representatives, while the EU Parliament representatives have no voting rights. In principle, the Court of Justice of the EU (CJEU) would have jurisdiction over Frontex's actions, but it has so far systematically avoided its responsibility by highlighting the Agency's "mere coordinating" function[45]. However, as we have seen above, Frontex has gained considerable operative power over time, making the CJEU's stance increasingly untenable. Furthermore, Frontex has been tasked with running the ETIAS, the latest European database, which is expected to become operational in 2026. ETIAS will be based on travellers' risk assessment, a pre-emptive security approach which, as we have seen, is fundamentally at odds with the rule of law[46]. This makes it more urgent than ever to impose stronger accountability, democratic scrutiny, and effective judicial control over the agency. Against this backgorund, framing and addressing migration as a hybrid threat is more likely to hinder than facilitate this desirable development. Moreover, the problem, although exacerbated by the existing lack of controls over Frontex, is not confined to this agency. National states are also increasingly framing migration as a hybrid attack to justify the infringement of basic human rights[47].

Whilst the framing of migration as a hybrid threat primarily poses problems in terms of the rule of law, dealing with disinformation as a hybrid threat especially puts pressure on democratic principles. Paradoxically, the main cause for concern regarding disinformation is its potential to disrupt democratic processes and discourses. However, classifying disinformation as a hybrid threat could undermine the very principles that should be safeguarded. As Hannah Arendt insightfully argued, claims to absolute "truth" and validity are contrary to the essence of political discourse. The political sphere thrives on debate, discussion and the exchange of opinions. On the other hand, Arendt also observed that all very different opinions must have a place in political discourse and are legitimate as long as they respect the integrity of the facts to which they refer[48]. As Arendt reminds us, protecting the democratic sphere by ensuring participation in public discourse and the exchange of diverse opinions, while anchoring these in the integrity of facts, is an arduous task requiring a nuanced approach in which criticism, openness, and diversity of opinion are essential. Exceptionalism and existential threats, on the other hand, are the most effective ways to silence criticism and differing opinions. Therefore, it is highly unlikely that democracy can be best defended under the banner of fighting "hybrid threats".

5. Conclusion

This article examined the increasing tendency within the EU to categorise issues as "hybrid threats" and investigated the impact of this on security understanding and practices. It analysed the cases of migration and disinformation in particular. Once these phenomena had been "securitised", meaning they were declared and dealt with as security problems, the hybridisation of security shifted EU measures in this area towards the "existential threat" extreme by interlacing the civil/internal and military/external spheres. These developments exacerbate the existing problems of lack of accountability and democratic control within the EU, making the need to strengthen power-restricting mechanisms and democratic participation more urgent than ever.

---

45. DE CONINCK 2023.

46. Specifically on Frontex and ETIAS see THÖNNES–VAVOULA 2023; EKLUND 2022.

47. BÜCKER–MÖLLER 2025.

48. ARENDT 1964/2013, pp. 23-27.

References

L. Amoore (2011), *Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times*, in "Theory, Culture & Society", vol. 28, 2011

H. Arendt (1964/2013), *Wahrheit und Lüge in der Politik: Zwei Essays*, Piper Taschenbuch, 2013

E. Bayamlıoğlu, R. Leenes (2018), *The 'rule of law' implications of data-driven decision-making: a techno-regulatory perspective*, in "Law, Innovation and Technology", vol. 10, 2018

R. Bellanova, M. de Goede (2020), *The Algorithmic Regulation of Security: An Infrastructural Perspective*, in "Regulation & Governance", 2020

D. Bigo (2002), *Security and Immigration: Toward a Critique of the Governmentality of Unease*, in "Alternatives 27", Special Issue, 2002

D. Bigo (2000), *When two become one: Internal and external securitisations in Europe*, in "International Relations Theory and the Politics of European Integration", Routledge, 2000

K. Bleyer-Simon, M.A. Horowitz, M. Botan et al. (2025), *How Is Disinformation Addressed in the Member States of the European Union? – 27 Country Cases*, in "European Digital Media Observatory", 2025

J. Bücker, L.S. Möller (2025), *Beyond Derogation: Context-Driven Interpretation of Migrants' Rights and the Risks of Circumventing Article 15 ECHR*, in "Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper", vol. 6, 2025

B. Buzan, O. Wæver (2003), *Regions and Powers: The Structure of International Security*, Cambridge University Press, 2003

A. Casero-Ripollés, J. Tuñón, L. Bouza-García (2023), *The European Approach to Online Disinformation: Geopolitical and Regulatory Dissonance*, in "Humanities and Social Sciences Communications", vol. 10, 2023

J. De Coninck (2023), *Shielding Frontex*, in "Verfassungsblog", September 2023

H. de Waele (2017), *Entrenching the Area of Freedom, Security and Justice. Questions of institutional governance and judicial control*, in M. Fletcher, E. Herlin-Karnell, C. Matera (eds.), "The European Union as an Area of Freedom, Security and Justice", Routledge, 2017

M. den Boer (2008), *Immigration and its Effect on the Security Discourse in Europe: Time for Demystification*, in "Amsterdam Law Forum", vol. 1, 2008, n. 1

A.M. Eklund (2022), *Frontex and 'Algorithmic Discretion' (Part I): The ETIAS Screening Rules and the Principle of Legality*, in "Verfassungsblog", September, 2023

S. Ellebrecht (2020), *Mediated Bordering:* EUROSUR, *the Refugee Boat, and the Construction of an External EU Border*, transcript publishing, 2020

European Commission (Directorate-General for Communications Networks, Content and Technology) (2018), *A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation*, Publications Office, 2018

B. Frischmann, E. Selinger (2018), *Re-Engineering Humanity*, Cambridge University Press, 2018

G. Giannopoulos, H. Smith, M. Theocharidou (2021), *The Landscape of Hybrid Threats: A Conceptual Model (Public Version)*, Publications Office of the European Union, 2021

M. Hildebrandt (2018), *Algorithmic regulation and the rule of law*, in "Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences", vol. 376, 2018

M. Hildebrandt (2016), *Law as Information in the Era of Data-Driven Agency*, in "The Modern Law Review", vol. 79, 2016, n. 1

M. Hildebrandt, A. Rouvroy (eds.) (2011), *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2011

R.L. Holzhacker, P. Luif (2014), *Introduction: Freedom, Security and Justice after Lisbon*, in Id. (eds.), "Freedom, Security, and Justice in the European Union: Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty", Springer, 2014

C. Kaunert, S. Léonard (2023), *Collective securitization and crisification of EU policy change two decades of EU counterterrorism policy*, Routledge, 2023

M. Leese (2014), *The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union*, in "Security Dialogue", vol. 45, 2014, n. 5

S. Léonard (2010), *EU border security and migration into the European Union: FRONTEX and securitisation through practices*, in "European Security", vol. 19, 2010, n. 2

S. Léonard, C. Kaunert (2022), *The securitisation of migration in the European Union: Frontex and its evolving security practices*, in "Journal of Ethnic and Migration Studies", vol. 48, 2022, n. 6

S. Lucarelli, J. Sperling, M. Webber (eds.) (2020), *Collective Securitisation and Security Governance in the European Union*, Routledge, 2020

V. Mitsilegas (2020), *The Preventive Turn in European Security Policy: Towards a Rule of Law Crisis?*, in F. Bignami (ed.), "EU Law in Populist Times: Crises and Prospects", Cambridge University Press, 2020

V. Mitsilegas (2015), *The Transformation of Privacy in an Era of Pre-emptive Surveillance*, in "Tilburg Law Review", vol. 20, 2015, n. 1

J. Monar (2001), *The Dynamics of Justice and Home Affairs: Laboratories, Driving Factors and Costs*, in "JCMS: Journal of Common Market Studies", vol. 39, 2001, n. 4

C. O'Neil (2016), *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Publishers, 2016

E. Orrù (2022-a), *Freedom, security and justice in the European Union: a short genealogy of the "Security Union"*, in "Eunomia. Rivista di studi su pace e diritti umani", 2022, n. 1

E. Orrù (2022-b), *Legittimità e digitalizzazione. Per una critica realistica delle politiche di sicurezza dell'Unione europea*, Wolters Kluwer, 2022

E. Orrù (2022-c), *The European PNR Directive as an Instance of Pre-Emptive, Risk-Based Algorithmic Security and Its Implications for the Regulatory Framework*, in "Information Polity", vol. 27, 2022, n. 2

E. Orrù (2021), *Legitimität, Sicherheit, Autonomie. Eine philosophische Analyse der EU-Sicherheitspolitik im Kontext der Digitalisierung*, Nomos, 2021

S. Peers (2017), *The rise and fall of EU justice and home affairs law*, in M. Fletcher, E. Herlin-Karnell, C. Matera (eds.), "The European Union as an Area of Freedom, Security and Justice", Routledge, 2017

R. Poscher (2016), *Tendencies in Public Civil Security Law*, in "European Journal for Security Research", vol. 1, 2016

J. Raz (1977), *The rule of law and its virtue*, in "Law Quarterly Review", vol. 93, 1977

A. Sarantaki (2023), *Frontex and the rising of a new border control culture in Europe*, Routledge, Taylor & Francis Group, 2023

E. Sason, C. Monti, P. Olivares-Martinez (2025), *Security – A Firm Construct or an Undetermined Concept?*, in "eucrim", 2025, n. 1

J. Sperling, M. Webber (2017), *NATO and the Ukraine Crisis: Collective Securitisation*, in "European Journal of International Security", vol. 2, 2017, n. 1

C. Thönnes, N. Vavoula (2023), *Automated Predictive Threat Detection after Ligue Des Droits Humains: Implications for ETIAS and CSAM (Part II)*, in "Verfassungsblog", 2023

L. Ulbricht (2018), *When Big Data Meet Securitization. Algorithmic Regulation with Passenger Name Records*, in "European Journal for Security Research", vol. 3, 2018

K. Yeung (2018), *Algorithmic Regulation: A Critical Interrogation*, in "Regulation & Governance", vol. 12, 2018