Public Governance, Administration and Finances Law Review Vol. 10. No. 1. (2025) • 33–42.

DOI: 10.53116/pgaflr.7939

Speech as "Hybrid Warfare"

Vincenzo Zeno-Zencovich*

* Full Professor of Comparative Law, Roma Tre University, Rome, Italy, e-mail: vincenzo.zenozencovich@uniroma3.it

Submitted: 25 January 2025 | Accepted: 05 June 2025 | Published online: 27 June 2025

Abstract: Long ago one used to say: "In a war truth is the first casualty." The saying now should go: "In a modern war the first shot is a speech." This paper wishes to point out how, over the last decade, informational activities have been classified as a form of "hybrid warfare" that should be countered and defeated. It analyses how traditional propaganda is now qualified as hybrid warfare and what are its consequences under international law, what does one mean for "disinformation" or "misinformation", and how and who can determine it, as well as what are the consequences of the weaponisation of informational activity in a democratic system and in its public debate. The paper argues that a hybrid warfare is a catch-all expression which can include any kind of activity deemed as "hostile" by a country, the notion of disinformation is misleading and fuzzy, and is apt to include any sort of speech, from simple facts to statements of opinion, finally, the emphasis on hostile speech as a form of hybrid warfare has a spillover effect in domestic public debate with a powerful silencing effect on non-conventional views.

Keywords: disinformation, DMA, DSA, free speech, hybrid warfare, misinformation

1. Hybrid warfare and hostile speech in the international arena

Words are important, especially in a legal context, and even more when the topic is free speech. A signal of the troubled times we live in is the surge of the term hybrid warfare in public debate. Hybrid warfare has several edulcorated synonyms, such as "gray zone", "asymmetric war", "non-linear war", "ambiguous warfare", or even "soft war" (for a comprehensive overview see Casey-Maslen, 2024). Some years ago, it was one of the expressions common in the Western military and security jargon (see NATO, 2024; Casey-Maslen, 2024, p. 6; Hoffman, 2018), being a deliberately vague expression[1] which

[1] See the authoritative statement by the NATO Assistant Secretary General Sorin D. Ducaru (2016, pp. 9–10): "There is so far no agreed definition of Hybrid Warfare within NATO taxonomy." "The Assembly notes that there is no universally agreed definition of 'hybrid war' and there is no 'law of hybrid war'. However, it is commonly agreed that the main feature of this phenomenon is 'legal asymmetry', as hybrid adversaries, as a rule, deny their responsibility for hybrid operations and try to escape the legal consequences of their actions. They exploit lacunae in the law

encompassed a series of actions which could not fall under the definition set by international treaties, noticeably Article 2(4) of the UN Charter.[2] The military and diplomats were asking themselves when the border of a formal "armed attack" (which allows self-defence according to Article 51 of the UN Charter) had occurred with all the consequences that such an attack would imply (see Ronzitti, 2021, p. 23; Casey-Maslen, 2024, p. 21).

However, in the last decade hybrid warfare has become a cat out of the box. The term is commonly used in official documents, in political speeches and in the media (see Galeotti, 2022, p. 11). The adjective "hybrid" is downplayed. The noun "warfare" is emphasised, also because "adversaries use the manifestation of cyber and info-warfare as an 'operational continuum'", that is war by other means (Ducaru, 2016, p. 21). Today, practically any action (or inaction) put into place, directly or indirectly, by another country, and which is considered hostile, falls under the notion of hybrid warfare. It "combines military and non-military tools in a deliberate and synchronised campaign to destabilise and gain *political leverage* over an opponent" (Ducaru, 2016, p. 10, italics added). "Hybrid warfare encourages instability in a country's internal affairs by prioritizing non-kinetic military methods such as cyber acts, influence over operations in coordination with economic pressure, support for local opposition groups, disinformation, and criminal activity" (Jovanovski, 2021, p. 152). Some situations can be considered quite novel, such as hostile activity which can be qualified as "digital", and the domain of cybersecurity covers a broad field encompassing all aspects of a country, whether in the public or in the private domain, and quite appropriately telecommunication networks are qualified as critical infrastructures.[3]

Nevertheless, other conducts are centuries old, and did not fall under the "act of war" definition. Among them one of the most common was "propaganda", a term whose meaning has changed over the decades (see Fridman et al., 2018). But in this context, one may encounter the notion of cognitive warfare as well, which is described by NATO as follows:

> Cognitive Warfare includes activities conducted in synchronization with other Instruments of Power, to affect attitudes and behaviours, by influencing, protecting, or disrupting individual, group, or population level cognition, to gain an advantage over an adversary. Designed to modify perceptions of reality, whole-of-society manipulation has become a new norm, with human cognition shaping to be a critical realm of warfare.

---

and the complexity of legal systems, operate across legal boundaries and in under-regulated spaces, exploit legal thresholds, are prepared to commit substantial violations of the law and generate confusion and ambiguity to mask their actions" (Council of Europe Parliamentary Assembly, 2018, point 5).

[2] But what exactly is an "act of war"? "It would seem to follow that an act of war is either intended by the actor State to bring about a condition of war or, though not so intended, may be regarded by the State against which it is directed as having done so" (Grant & Barker, 2009). With reference to hybrid warfare, see the analysis of the International Court of Justice case law in Fogt (2021).

[3] It is sufficient to mention the NATO's Cooperative Cyber Defence Centre of Excellence based in Tallinn and the host of publications it has promoted and collected, from the Tallinn Manual (https://ccdcoe.org/research/tallinn-manual) to the dedicated webpage (https://ccdcoe.org/incyder-articles/?year=2024).

> Cognitive Warfare focuses on attacking and degrading rationality, which can lead to exploitation of vulnerabilities and systemic weakening. However, this becomes increasingly complex as non-military targets are involved. An example: Russian social media and public information operations targeted much of the international community in an attempt to label Ukraine as being at fault. Through a combination of communication technologies, fake news stories, and perceptions manipulation, Russia aims to influence public opinion, as well as decay public trust towards open information sources. These narratives have extensive reach, and often involve both offensive and defensive posturing (NATO Allied Command Transformation, s. a.).

China, as a strategic competitor for NATO, describes Cognitive Warfare as the use of public opinion, psychological operations and legal influence to achieve victory. Combat psychology has significant impact on the warfighter's ability to function; the Intelligent Psychological Monitoring System, a recent smart sensor bracelet developed by China, focuses on recording facial information, emotional changes, and psychological states of soldiers to determine their combat status. Outside of the battlefield, influence can also affect law, rule-of-order, and civil constructs. This inclusion of "Lawfare" and the targeting of broader community sentiment has significant impact, since so many civilians and non-combatants are potentially exposed.

Nevertheless, there are several critical issues which are opened by qualifying foreign propaganda as hybrid warfare, that is, "[t]aking advantage of the opportunities of cyberspace as a domain for free, fast and effective communication and to transform it into an efficient tool for [...] propaganda, manipulation and distortion of information, deception, information warfare" (Ducaru, 2016, p. 16; see Rühle, 2021).

First, as it belongs to any given state to establish what is considered an act of war, of necessity it is to the given state to decide if propaganda is a form of hybrid warfare. Clearly, this is a field in which the *raison d'état* governs, and there is little room for constitutional concerns (see Fogt, 2021). The consequence is that what is considered hostile is, ultimately, a political, and politically oriented, decision.[4]

Second, qualifying it as hostile speech, a synonym for propaganda, hybrid warfare obviously trumps all international agreements[5] which were meant to favour free circulation of news, opinions and ideas.[6] And as hybrid warfare includes actions by non-state actors, the silencing effect is without any subjective limitations.

---

[4] "The wide array of possible elements included in a hybrid attack requires a 'whole of government' response that combines all national instruments." (Ducaru, 2016, p. 12) "A hybrid information campaign, psychological operations, or any other hostile informational activity regarding fake news will not reach the threshold of an armed conflict in the sense of an armed attack or equivalent acts of aggression, but may still constitute an unlawful threat of attack or other unlawful acts under international law such as interfering in the internal affairs of other states" (Fogt, 2021, p. 97).

[5] The first reference is to the Final Act of the 1975 Helsinki Conference on Security and Co-operation in Europe which devoted a section to transborder flow of information stating that the signatory States "[m]ake it their aim to facilitate the freer and wider dissemination of information of all kinds, to encourage co-operation in the field of information and the exchange of information with other countries".

[6] Which is quite obvious if you include in hybrid warfare actions aimed at "generate deception and ambiguity" and "avoid attribution of action; maximize deniability of responsibility for aggressive actions" (Ducaru, 2016, p. 10).

And third, as one of the tenets when facing hybrid warfare is that of "deterring" it,[7] the inescapable consequence is that of preventive censorship. Once hostile speech has entered the country, it is useless to counter it.[8] This implies that the medium through which such messages are disseminated must be blocked at its source. There is no room for a case-by-case analysis. Even a weather report or sports might conceal covert disruptive contents.[9] From a Western legal tradition perspective, this approach, which has been consistently followed by the EU after the Russian invasion of Ukraine,[10] has two significant consequences. In the first place, it disenfranchises conducts by any other country which consider communication coming from the West as a hostile interference in their internal affairs.[11] The most obvious victim is any propaganda in favour of human rights. And the second is that Western democracies engage in practices that over the last eight decades have been flagged as typical indicators of a dictatorship, ensuring its stability by denying its citizens access to foreign sources.[12]

2. The domestic spillover effects of hybrid warfare

The most critical aspect of the weaponisation of speech is the internal effects that the hybrid warfare rhetoric brings with it. These effects only in a limited measure curtail access to foreign information sources.[13] To express the notion in very practical terms, and to place in our contemporary troubled times, it equalises internal propaganda to foreign one, and freezes any critical debate on whether the West has some political and

[7] "The Triad: Prepare–Deter–Defend" (Ducaru, 2016, p. 13).

[8] For the most part, counter information measures will have to be strictly based on facts and truth and will, thus, come too late to prevent the effect of the hybrid campaign – the countermeasures will only mitigate the damages" (Fogt, 2021, p. 97).

[9] This is because "a hybrid threat or warfare conducted by overt or covert activities by states, state agents or non-state actors in times of peace, crisis or armed conflict will affect the full-spectrum of the society of the targeted state" (Fogt, 2021, p. 31).

[10] The most significant expression of it is the EU Council conclusions (21 June 2022) on a Framework for a coordinated EU response to hybrid campaigns (European Council, 2021).

[11] Typically, the "use of 'lawfare' in terms of promoting one's own actions as legitimate and opponents' reactions as unlawful" (Fogt, 2021, p. 33).

[12] Can one still speak of "asymmetry" between democratic and non-democratic countries? "The opportunities to utilize disinformation have therefore increased, and they are especially attractive to authoritarian regimes. This also results in an inherent asymmetry. While influence efforts targeting foreign target audiences can benefit from the openness of democratic societies, authoritarian states can implement restrictions in their own domestic information environment, delimiting communication between their own population and external actors" (Weissmann et al., 2021, p. 120).

[13] The reference is, obviously to the Decision taken on 27 July 2022 by the Grand Chamber of the EU General Court in the *Russia Today v. Council* case (T-125/22). For some critical comments, see Ó Fataigh & Voorhoof (2022, p. 186), Sassi (2022, p. 1253) and Zeno-Zencovich (2024, p. 175).

military responsibilities in favouring the Russian aggression against Ukraine,[14] a debate which in no way is meant to justify a blatant violation of international law, but questioning the frequent practice of "double standards" by righteous Western democracies (see e.g. Saul, 2022). However, the effects go well beyond the dramatic geopolitical situation in Eastern Europe, and strengthen a growing tendency to regulate speech.

The first step is to qualify as hostile any speech which purportedly is against a long list of "values".[15] Values are, therefore, placed in a dogmatic, quasi-religious context which should not be countered by speech. This means putting back the clock to the ages which one imagined past when expressing views not approved by the public authorities brought exclusion, banishment, imprisonment and, often, physical elimination. This is because a speech which is not accepted is immediately linked to the author, with a stigmatising effect. A speech is not analysed and discussed but it is simplistically labelled as proper or improper. The author is, therefore, classified as belonging to a certain group that should be countered (on the abuse of labelling see Friedland, 2024).

A political and constitutional freedom, free speech, becomes the rostrum for self-incrimination. One is judged not for one's acts but for one's words. This is not to advocate a society imbued with hypocrite politesse but to point out how "internal enemies" are created. Clearly one's reputation is made also by what one expresses, however, the significant element in the European Union's approach is that of creating categories of not-accepted speech. This is done through non-state agents outsourcing control over speech by private actors. This is because on the one hand states are not able technically to detect speech that falls into not-accepted categories. On the other hand, this form of censorship, which clearly would not be legally admissible if put into place by the state, is downsized as simple non-compliance with contractual obligations.

To put the extensive normative provision, contained in Articles 34, 35 and 36 of the Digital Services Act (DSA) briefly,[16] the "very large online platforms" will have to put in algorithmic systems that prevent "the dissemination of illegal content through their

[14] See how the news of a further clamp-down on Russian media outlets is given by the EU Commission: "The Commission welcomes the Council decision to suspend the broadcasting activities of four more media outlets (Voice of Europe, RIA Novosti, Izvestia and Rossiyskaya Gazeta) in the EU or directed at the EU, in view of their role supporting and justifying Russia's war of aggression against Ukraine. Russia has engaged in continuous and concerted propaganda as well as information manipulation actions targeted at civil society in the EU and neighbouring countries, gravely distorting and manipulating facts. These propaganda actions have been channelled through a number of media outlets under the permanent direct or indirect control of the leadership of the Russian Federation. Such actions constitute a significant and direct threat to the Union's public order and security. The risk to our democratic societies – and the integrity of the upcoming European as well as national elections – has intensified. Today's measures are a forceful response to that. The sanctions do not target freedom of opinion. They include specific safeguards for freedom of expression and journalistic activities. The measures do not prevent the sanctioned outlets and their staff from carrying out other activities in the Union other than broadcasting, such as research and interviews. The measures should be maintained until the aggression against Ukraine is put to an end, and until the Russian Federation and its associated outlets cease to conduct disinformation and information manipulation actions against the EU and its Member States" (European Commission, 2024).

[15] "Disinformation", both foreign and domestic, is listed as one of the most relevant "hybrid threats" in the Communication from the Commission to the European Parliament and the Council on "ProtectEU: A European Internal Security Strategy". Strasbourg, 1.4.2025, COM(2025) 148 final.

[16] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.

services", which is not only a legal obligation, but also an economic decision.[17] One has already experimented the results, often ludicrous, of such algorithmic screening that have erased from the internet breast-feeding Madonnas, *putti,* paintings and sculptures of Venus, towns and people whose name fell into the politically incorrect, primitive vocabulary of Facebook,[18] and the frequent suspension of email or other personal communication services through the detection of messages and photographs which the algorithm considers inappropriate.[19] The very large online platforms are, therefore, entrusted with a policing role that public authorities are not able to perform. In substance, a fundamental right such as that of expression that in our technological environment can be put into practice only through the internet and intermediary services and platforms will be subject to algorithmic preventive censorship.[20]

The DSA puts together extremely different phenomena: terrorist content, child pornography, "illegal racist and xenophobic expressions". But if one extends the scope to the vast area of "discriminatory speech", which falls within the "otherwise harmful" category, one can already see the multitude of organisations which, purporting the defence of minority groups, ask for the removal of speech or other forms of expression which they consider offensive. It is sufficient to look at the aggressive campaigns conducted under the flags of trans-Atlantic movements ("Me-Too", "Cancel Culture",[21] "Black Lives Matter", "Last Generation", LGBTQ+, etc.) to understand what the effects of such private internet militia can be on freedom of expression.[22] Clearly, the very large online platforms, in order to avoid heavy administrative and financial sanctions, draft lengthy terms and conditions which apply to all individual users of the platform.

These terms and conditions set also limits on the content of online speech. If they were not binding and algorithmically enforced, the "community standards" of Meta, together with its endless list of forbidden words and ideas, would be considered ludicrous.

---

[17] "[A] significant number of platform legal interpretations are incorrect. These divergent interpretations of the law mean that we believe platforms are removing legal content that they falsely believe to be illegal ('over-blocking') while simultaneously not moderating illegal content ('under-blocking')" (Wagner et al., 2024, p. 2).

[18] For those who have the time, it is suggested to browse the endless index of forbidden words and expressions in the various chapters of Facebook's "community standards", for example, violence and criminal behaviour, coordinating harm and promoting crime, dangerous organisations and individuals, fraud and deception, violence and incitement, etc.

[19] In the U.S. context, "*ex ante* AI-based content moderation operates in much the same way as a prior restraint; like government prepublication censorship, it gives users no notice of takedowns prior to publication, nor reasons for the takedown decision (at least reasons that a lay user would be capable of understanding)" (Armijo, 2021, p. 245).

[20] The point is thoroughly examined and challenged by Vigevani (2023). The obvious conclusion is that such practices "only benefit social media platforms in the sense that they allow the platforms to strengthen their position as private regulators of online freedom of expression through their own unilaterally adopted rules and for the benefit of their business model" (Cetina Presuel, 2021, p. 499).

[21] It is worth noting that recently Italy has introduced an amendment to the Audiovisual Media Services Law (Decree 25.3.2024. n. 50) which establishes that audiovisual media providers, while respecting human dignity and combating "hate speech" [Article 4(1)(b)], should oppose "contemporary tendencies to destroy or anyway belittle the elements or the symbols or of the tradition of the Nation (cancel culture)" [Article 4(1)(h)]. Apart from the rather haphazard definition of cancel culture, it is doubtful that legal norms can effectively counter a phenomenon that most clearly is the product of ignorance and fanatism.

[22] Obviously there are authors who, quite at the opposite, welcome the DSA for imposing on the very large platforms the respect of fundamental rights. This would enhance speech by "minority and marginalized groups" (see e.g. Quintais et al., 2023).

No public institution would ever dream of setting such rules, and if challenged, they would never pass judicial scrutiny being vague, overbroad and lacking any proportionality. The state establishes what can, and what cannot be said, such as hate speech, discriminatory speech, speech which expresses a gender, sexual, racial, ethnical, geographical, ideological bias. An index of forbidden words is placed upon public institutions, law enforcement, courts, educational institutions or non-private actors.

In the international arena "hostile speech" is a form of hybrid warfare. In the domestic one, what is engaged in a "war" (this is the term most commonly used) on "harmful speech" which must be prevented. Just as the state establishes what is hostile, it establishes what is harmful.[23] Facts, opinions, ideas are placed in the battleground and classified as friends or foes, the preliminary step is to establish which general topic of discussion are under surveillance, then to set certain periods in which speech must be restrained (typically: elections), finally to control the medium. While the two processes go hand in hand, the internal weaponisation of speech inasmuch as it limits the constitutional rights of all citizens, requires that there can hardly be room for *raison d'état,* the limit being that, important but not over-reaching, of state secrets. Censorship and gag-orders are clearly inadmissible. A black-and-white *ex ante* vision, is substituted by an *ex post* balancing test; the courts, and not the government (or its private proxies), are entrusted with the policing of speech.

There is no doubt that such a system presents many flaws especially if one looks at its effectiveness. But it should be questioned that one can apply dubious categories of international relations and conflicts to "uninhibited, robust, and wide-open" debate in a democracy. The internalisation of the hybrid warfare discourse passes through two steps, one substantive, the other procedural. The best example is provided by the recent European Media Freedom Act (EMFA) of the EU.[24] Its purported aim is, *inter alia,* that of protecting the "Fortress Europe" from its external enemies. The text is strewn with references to such foes: in multiple Recitals (4, 6, 53) reference is made to "providers, including those controlled by certain third countries, that systematically engage in disinformation or information-manipulation".

The link between hybrid warfare and information activity is made forcefully in other recitals of the EMFA which stress the need to contrast "foreign information manipulation and interference" (14, 74). And denounce as a threat "systematic campaigns of foreign information manipulation and interference with a view to destabilizing the Union as a whole or particular Member States" (Recital 47). This imposes the duty to "protect users from foreign information manipulation and interference" (Articles 19 and 26). Having equated external and internal disinformation as forms of interference, the necessary step is that of defining what forms of speech must be contrasted and blocked. The "golden

[23] Even more troubling is the Media Freedom Act [Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU] which in its Recital 4 targets the "polarizing content".

[24] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU.

book" is the Strengthened Code of Practice on Disinformation 2022 which again equates "misinformation", "disinformation", "information influence operations"[25] and "foreign interference".[26]

In the first place, it is striking that a fundamental right such as freedom of expression is, at the bottom line, regulated by a sub-sub-sub primary source, the European Commission's 2021 Communication on the European Democracy Action Plan, which openly affirms the contiguity of external and internal informational activities. The Strengthened Code translates these tenets into a would-be self-regulatory instrument. But as one has learnt from the past, it is simply a camouflaged form of regulation in an area which manifestly is and should be outside the competences that the EU Treaties have conferred upon the Commission. What speech can be qualified as disinformation? As they are in the habit, the EU institutions subvert traditional legal logic.

A new category is created, that of "harmful content", "harmful campaigns", "harmful disinformation". What is harmful is decided not by a court but by organised groups or single individuals who "flag" the content they object to according to their preferences, ideology, or idiosyncrasies. Compliance with the fuzzy notions of the Strengthened Code is imposed by the mastodontic DSA which repeatedly targets "otherwise harmful information" (Recital 5) "otherwise harmful content" (Recital 68) and sanctions both Internet providers and "very large online platforms" which do not remove such content. Especially the very large online platforms are subject to multiple obligations, which can be complied with only through an algorithmic surveillance (made even more effective through AI) of what is disseminated on the web.

3. Conclusion

One can detect a continuum which from the international arena moves towards the domestic arena with dramatic consequences on the notion itself of "free speech". The EU while paying lip-service to fundamental rights, first of all freedom of expression, is gradually introducing legal instruments (whether through legislation or through court decisions) whose effect is that of stifling views that do not conform to its dominant ideology. This is troublesome because one can – and probably should – have serious doubts that these interventions on free speech fall within the remit of the Treaties and the legitimate prerogatives of the EU institutions.

[25] Defined as "information influence operation refers to coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation".

[26] Defined as "foreign interference in the information space, often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents".

Acknowledgments

The author is grateful to Professor Giulio Bartolini whose assistance was of invaluable help in correcting a series of flaws in the first draft of this paper.

References

Armijo, E. (2021). Speech Regulation by Algorithm. *William & Mary Bill of Rights Journal, 30*(2), 245–263. Online: https://scholarship.law.wm.edu/wmborj/vol30/iss2/3

Casey-Maslen, S. (2024). *Hybrid Warfare under International Law.* Hart Publishing. Online: https://doi.org/10.5040/9781509979608

Cetina Presuel, R. (2021). Un estira y afloja: La definición de las reglas para la libre expresión en las plataformas de redes sociales. *Jurídicas CUC, 17*(1), 499–556. Online: https://doi.org/10.17981/juridcuc.17.1.2021.18

Council of Europe Parliamentary Assembly (2018). *Resolution 2217. Legal Challenges Related to Hybrid War and Human Rights Obligations.* Online: https://tinyurl.com/44xk6jbd

Ducaru, S. D. (2016). The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO. *Europolity, 10*(1), 7–23. Online: https://tinyurl.com/zzdhwpew

European Commission (2024, May 17). *Commission Welcomes New Sanctions against Disinformation and War Propaganda.* Online: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2682

European Council (2021, June 21). *Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns.* Online: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns

Fogt, M. M. (2021). Legal Challenges or 'Gaps' by Countering Hybrid Warfare. Building Resilience in *Jus ante Bellum*. *Southwestern Journal of International Law, 27*(1), 28–100.

Fridman, O., Kabernik, V. & Pearce, J. C. (Eds.). (2018). *Hybrid Conflicts and Information Warfare. New Labels, Old Politics.* Lynne Rienner.

Friedland, S. (2024, June). *Speech Labels and Bias.* Paper presentation. Free Speech Discussion Forum in Budapest, 13–14 June, 2024, Budapest.

Galeotti, M. (2022). *The Weaponisation of Everything. A Field Guide to the New Way of War.* Yale University Press. Online: https://doi.org/10.2307/j.ctv28bqm27

Grant, J. P. & Barker, J. C. (2009). *Parry and Grant Encyclopaedic Dictionary of International Law.* 3rd ed. Oxford University Press. Online: https://doi.org/10.1093/acref/9780195389777.001.0001

Hoffman, F. G. (2018). Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *Prism, 7*(4), 30–47.

Jovanovski, Z. (2021). Challenges of International Humanitarian Law in Regulating Conflicts from the Era of Hybrid Warfare. *Balkan Social Science Review, 18,* 149–167. Online: https://doi.org/10.46763/bssr2118149j

NATO (2024, May 7). *Countering Hybrid Threats.* Online: https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO Allied Command Transformation (s. a.). *Cognitive Warfare.* Online: https://www.act.nato.int/activities/cognitive-warfare/

Ó Fataigh, R. & Voorhoof, D. (2022). Freedom of Expression and the EU's Ban on Russia Today: A Dangerous Rubicon Crossed. *Communications Law, 27*(4), 186–193.

Quintais, J. P., Appelman, N. & Fahy, R. (2023). Using Terms and Conditions to Apply Fundamental Rights to Content Moderation. *German Law Journal, 24*(5), 881–911. Online: https://doi.org/10.1017/glj.2023.53

Ronzitti, N. (2021). *Diritto internazionale dei conflitti armati.* Giappichelli.

Rühle, M. (2021). NATO's Response to Hybrid Threats. In D. P. Jankowski & T. Stępniewski (Eds.), *NATO in the Era of Unpeace. Defending Against Known Unknowns* (pp. 59–80). Instytut Europy Środkowej.

Sassi, S. (2022). La soft war dell'Unione Europea: il caso RT-France c. Consiglio. *Il Diritto dell'informazione e dell'informatica, 38*(6), 1199–1259.

Saul, B. (2022, July). The Law of the Jungle: Western Hypocrisy over the Russian Invasion of Ukraine. *Australian Book Review,* (444). Online: https://tinyurl.com/26y8z3zd

Vigevani, G. E. (2023). Piattaforme digitali private, potere pubblico e libertà di espressione. *Rivista di diritto costituzionale, 61*(1), 41–54.

Wagner, B., Kettemann, M. C., Tiedeke, A. S., Rachinger, F. & Sekwenz, M.-T. (2024). Mapping Interpretations of the Law in Online Content Moderation in Germany. *Computer Law & Security Review, 55.* Online: https://doi.org/10.1016/j.clsr.2024.106054

Weissmann, M., Nilsson, N., Palmertz, B. & Thunholm, P. (Eds.). (2021). *Hybrid Warfare. Security and Asymmetric Conflict in International Relations.* I.B. Tauris. Online: https://doi.org/10.5040/9781788317795

Zeno-Zencovich, V. (2024). The EU's Regulation of Speech: A Critical View. *University of the Pacific Law Review, 55*(2), 175–183.