Techade: An International e-Journal on Emerging Technologies and Power Dynamics
Vol. 2, Issue 1 | June 2026

Artificial Intelligence, Climate Disinformation, and Counter-Securitisation: Russian Hybrid Warfare Targeting European Union Climate Policy

Abinay Rai,[i] Dr Ram Babu,[ii] and Rahul Kumar Tiwari[iii]

Abstract

Russian disinformation about climate change increasingly functions as an extension of hybrid warfare against the European Union, rather than a standalone campaign against climate science. This paper asks how Russian and Russian-aligned actors use artificial intelligence (AI) to contest EU climate security, and when this counter-securitisation gains traction. Existing scholarship treats hybrid warfare, securitisation theory, and AI-enabled disinformation as separate literatures, often assuming AI-enabled disinformation operates as hybrid warfare without testing when it does. This paper develops a conditional model instead, arguing that contestation of EU climate security depends on the fit between narratives and domestic grievance, the evidentiary tier of Kremlin attribution, and AI's discursive rather than productive role. Using qualitative content analysis and narrative coding of Kremlin-aligned and obstructionist messaging, supported by network tracing, the paper compares three cases with uneven documentation depth: Bulgaria, Poland, and a joint France-Germany-Netherlands cluster. The analysis finds a dual-track Russian strategy combining physical disruption of energy infrastructure with narrative contestation of the green transition. Obstructionist networks vary structurally by case, from a concentrated Telegram cluster in Bulgaria to a diffuse, state-linked ecosystem in Poland, while confirmed generative-AI involvement remains limited to the France-Germany-Netherlands cluster. AI's contribution currently operates more through a discursive plausibility effect than through demonstrated production capacity. The paper contributes a conditional framework for AI-enabled counter-

securitisation and identifies gaps in EU disinformation governance, including the treatment of coordinated inauthentic behaviour under the Digital Services Act.

Keywords: Hybrid warfare; Climate disinformation; Counter-securitisation; AI-enabled disinformation; Obstructionist networks.

Introduction

Russian disinformation about climate change increasingly reads as an extension of the war against Ukraine rather than a separate campaign against climate science. Briggs and Matejova (2023) trace this connection to well before 2022: the Kremlin's assault on trust in energy transitions and climate expertise predates the invasion, which extended existing tactics rather than inventing new ones. Briggs (2020) had already argued, two years earlier, that hybrid warfare and climate security share more analytical ground than security planners typically assume, particularly through resilience targeting, information operations, and geoengineering. This paper takes that intersection as its starting point. It poses questions about how the intersection has evolved between the time periods from 2022 to 2026, as generative AI has become part of the disinformation toolbox and climate policy is increasingly being perceived as a security issue in the EU (Geri 2024).

Hybrid warfare research documents Russian disinformation, cyber activity, and economic coercion against European institutions in some detail. A resilience agenda, outlined by Kalniete and Pildegovics (2021) and Bajarunas (2020), is focused largely on cyber defence, strategic communication and whole-of-society preparedness, and was primarily developed in response to election interference and the attacks on infrastructure, not in relation to climate policy specifically. The current literature is extended by Geri (2024), who considers the linkage between energy, resources and decarbonisation as a new vulnerability that is the focus of Russian hybrid strategy. The term is not uncritically accepted by all scholars, partly because of NATO's adoption of the

term ‘hybrid warfare’, has become trendy, and is sometimes used politically (Libiseller 2023). EU institutions themselves have yet to reach a consensus on the boundaries between a hybrid operation, a hybrid campaign and a hybrid threat (Bazarkina 2022).

Another sets of literature, explains how climate change has turned into a security challenge for the EU. Securitisation theory understands this as a speech act, whereby an actor portrays an issue as a threat to existence and an audience adopts unusual responses to the threat (Baele and Jalea 2023). Morsut and Rhinard (2025) argued that the EU’s climate-security framing is not a script, but a recursive, evolving institutional settlement. Rhinard et al. (2023) further added that the member states are very different in their extent of securitisation of climate adaptation. Warner and Boas (2019) caution that securitising climate policy can backfire if audiences read the move as manipulative. A risk Baele and Jalea (2023) argue the wider literature has not tested carefully enough. These accounts explain how EU climate securitisation was built. They say comparatively little about how it is contested from outside.

A third body of work addresses that contestation, usually without reference to hybrid warfare theory. Galaz et al. (2023) describe a “perfect storm” in which engagement-driven algorithms, social bots, and generative AI combine to make climate misinformation cheaper to produce and harder to verify. Jackson et al. (2025) show that climate disinformation increasingly targets the politics of climate action rather than the underlying science, with implications that are geopolitical as much as domestic. What remains largely untested is how these three literatures, hybrid warfare, securitisation, and AI-enabled disinformation, fit together. Existing accounts tend to assert that AI-enabled climate disinformation functions as hybrid warfare against EU climate security, rather than examine the conditions under which this holds.

This paper addresses that gap through three linked research questions. First, how Russia links energy coercion, digital manipulation, and climate narratives within its hybrid warfare strategy, Second, which European obstructionist networks these narratives are localised and amplified, and third, when such campaigns weaken support for EU climate securitisation, and when EU institutions instead absorb the shock.

The paper's theoretical contribution is a conditional model of AI-enabled counter-securitisation. Rather than treating Russian and obstructionist narratives as straightforward climate denial, or as a uniformly effective hybrid warfare tool, the model specifies conditions under which contestation of EU climate security plausibly gains traction. These conditions include the fit between narratives and domestic grievance, the evidentiary tier of Kremlin attribution, and AI's discursive rather than purely productive role. This does not present a new alternative to existing hybrid warfare and securitisation framework, but rather it extends on those frameworks.

The paper's methodology follows a qualitative content analysis and narrative coding of Kremlin-aligned and obstructionist messaging, supported by network tracing of the actors that carry these narratives. It focuses on three cases with different depths of documentation, namely Bulgaria, Poland, and a joint France-Germany-Netherlands grouping. Evidence density varies notably across these cases, and this asymmetry is treated as a finding instead of brushed aside.

The paper further is organised as follows: Section two develops the theoretical framework linking hybrid and cognitive warfare, EU climate securitisation, and AI-enabled disinformation. Section three sets out the research design. Sections four and five present the empirical analysis, first of Russian narrative content and then of the obstructionist networks that carry it. Section six returns to theory, assessing how far securitisation and hybrid warfare concepts capture the empirical

patterns identified. Section seven concludes with policy implications for EU information governance and the study's limitations.

Theoretical framework

Hybrid and Cognitive Warfare: Concepts and Russian Application

Hybrid warfare is one of the most contested concepts in security studies. Hoffman introduced it in 2007 to describe the combination of conventional and irregular tactics, terrorism, and criminality within a single campaign. The term entered mainstream policy language only later, after NATO applied it to Russia's actions in Crimea and eastern Ukraine (Geri 202; Kalniete and Pildegovics 2021). In current use, the term refers to campaigns that combine diplomacy, information operations, cyber activity, economic coercion, and military pressure to weaken an opponent below the threshold of open war (Geri 2024; Bajarunas 2020). Cognitive warfare is the informational and psychological dimension of this strategy. It aims to divide societies, erode trust, and shape perception through disinformation, bots, and narrative manipulation (Kalniete and Pildegovics 2021).

Russia's application of these methods against Europe is well documented. The literature links Russian influence operations to Brexit interference, flight MH17 disinformation campaign, and broader efforts to finance or empower illiberal actors in Europe (Kalniete and Pildegovics 2021, 24; Geri 2024). Libiseller argues that hybrid warfare became fashionable after NATO's adoption of the term, which encouraged uncritical borrowing and politicized the academic debate (Libiseller 2023, 858–860). Bazarkina adds a further nuance: even within EU institutions, the boundary between "hybrid operation," "hybrid campaign," and "hybrid threat" remains poorly defined (Bazarkina 2022). This definitional looseness allows the label to be applied elastically. It can

describe genuine security concerns such as terrorism or cybercrime, but it can also justify economic measures against political and commercial rivals. That is not a neutral analytical gap. It is also a political problem, because the concept can be used to discipline adversaries rather than clarify threat environments.

For this paper, the key point is that Russian hybrid warfare is no longer limited to military coercion. It now reaches into the climate-energy domain, where Russia can exploit energy dependence, disrupt critical infrastructure, and weaken support for decarbonization (Geri 2024). That matters because hybrid warfare in Europe now includes not only territorial insecurity but also vulnerabilities created by the green transition and the supply chains that sustain it. The analytical task is therefore to trace how Russia uses non-kinetic pressure to turn climate and energy policy into a battlefield of legitimacy, trust, and resilience.

Securitization and Climate Security in the EU

Securitization theory explains why an issue is treated as existential rather than routine. In the Copenhagen School, securitization is a speech act through which an actor frames a threat and an audience accepts extraordinary measures in response (Baele and Jalea 2023). Climate change entered this security field through UN and EU debates in the late 2000s, when the EU framed it as a threat multiplier and embedded it into broader foreign, development, and resilience policy (Liberatore 2013). Later work distinguishes this from riskification, where climate is governed through expertise and anticipation rather than emergency language (Mees and Surian 2023). Rhinard et al. show that EU member states differ widely in how far climate adaptation is securitized, so the process is uneven rather than universal (Rhinard et al. 2023).

This matters for the present study because the EU's climate-security agenda is not a fixed ideological script. It is an evolving institutional settlement. Morsut and Rhinard show that

securitization is recursive: the EU borrows risk framing from the UN, then reintroduces threat language back into global debates (Morsut and Rhinard 2025). Dreyer and Holm argue that climate securitization can also be transformative, not only defensive, when crisis framing is used to justify durable institutional change (Dreyer and Holm 2025). Warner and Boas caution, however, that securitizing climate policy can backfire if audiences interpret the move as manipulative or instrumental (Warner and Boas 2019). Baele and Jalea similarly warn that securitization theory is under-tested relative to how often it is invoked (Baele and Jalea 2023).

Russian climate-energy narratives operate inside this contested space. They do not simply deny climate change. They challenge the legitimacy of the EU's institutional response, portraying climate policy as coercive, elitist, or economically destructive. The point is not to reverse climate science. It is to weaken the political conditions under which climate security becomes governable. The security implication is that counter-securitisation should not be understood as a rejection of climate security. It is a struggle over who defines the threat, who speaks for expertise, and which actors can convert crisis into durable policy authority (Rhinard et al. 2023; Morsut and Rhinard 2025).

AI-enabled climate disinformation and obstructionist networks

AI does not create climate disinformation from nothing. It amplifies a pre-existing ecosystem of bots, recommender systems, and synthetic content. Galaz et al. show that engagement-based algorithms reward sensational material, while generative AI makes it easier to produce text, images, audio, and video that appear credible but remain unverified (Galaz et al. 2023). Their broader synthesis describes a "perfect storm" of automation, platform opacity, and AI-generated content in climate misinformation (Galaz et al. 2023). The practical effect is not only scale. It is also persuasion, speed, and mimicry (Garcia-Faroldi et al. 2025; Jackson et al. 2025).

In this paper, "European obstructionist networks" refers to domestic and transnational intermediaries that translate and normalize Kremlin-linked narratives. They are not passive repeaters. They adapt messages to local grievances over energy prices, climate costs, sovereignty, and food security (Dzhekova et al. 2025; Grostern 2025). The Bulgarian case shows how pro-Kremlin outlets and Telegram channels linked the European Green Deal to economic collapse and anti-expert claims (Dzhekova et al. 2025). The Polish material summarized by DeSmog presents climate disinformation as part of a long-term cognitive war against climate science, the EU, and democratic trust (Grostern 2025). Starbird et al. help explain why this works: disinformation is collaborative work, not just top-down propaganda (Starbird et al. 2019).

The AI dimension sharpens the hybrid logic. Iampolsca argues that Russia's toolkit has moved from troll farms toward algorithmic exploitation and generative AI, increasing volume and realism while retaining older tactics (Iampolsca 2026). Public perceptions of AI reinforce the credibility effect, because many audiences already assume that AI helps manufacture fake news (García-Faroldi et al. 2025). EU governance research reaches the same conclusion from another angle: AI can harm democracy through profiling, targeting, bots, and deepfakes, so responses must combine transparency, risk management, and education rather than content removal alone (Cupac and Sienknecht 2024). Calderaro and Blumfelde further argue that EU digital sovereignty remains fragile because the Union lacks control over the technical stack that shapes information flows (Calderaro and Blumfelde 2022).

Integrated framework and propositions

This paper links four stages: Russian hybrid strategy, AI-enabled climate disinformation, European obstructionist networks, and contestation of EU climate securitization. Russia first exploits the energy-resources-climate nexus through coercion and disruption (Geri 2024; Hoeffler et al. 2024).

It then uses digital manipulation to frame the green transition as costly, coercive, or anti-national, while AI lowers the cost of producing and circulating persuasive falsehoods (Jackson et al. 2025; Galaz et al. 2023; Iampolsca 2026). Obstructionist networks localize these narratives and amplify them through platform ecosystems and aligned outlets (Dzhekova et al. 2025; Grostern 2025). The result is not climate denial in the older sense. It is counter-securitisation: a challenge to the legitimacy of the EU's climate-security settlement (Wendler 2023; Morsut and Rhinard 2025; Dreyer and Holm 2025).

The framework is recursive rather than linear. REPowerEU did not rupture the European Green Deal. It mostly reworked existing policy subsystems through coordinated investment and soft governance (Wendler 2023). That institutional stability makes the political struggle shift toward legitimacy, agenda salience, and trust in expertise (Baele and Jalea 2023; Warner and Boas 2019). Three propositions follow. First, as AI reduces the cost and increases the plausibility of climate disinformation, hostile actors find it easier to intensify obstructionist narratives across EU information ecosystems (Galaz et al. 2023; García-Faroldi et al. 2025; Cupać and Sienknecht 2024). Second, the stronger the local fit between Russian narratives and domestic grievances over prices, sovereignty, or transition costs, the more likely obstructionist networks are to amplify them (Dzhekova et al. 2025; Grostern 2025; Jackson et al. 2025). Third, the more EU climate policy is framed as a security response, the more hostile actors will contest its legitimacy through claims that decarbonization is elitist, coercive, or economically destabilizing (Wendler 2023; Dreyer and Holm 2025; Warner and Boas 2019).

From these propositions follow three research questions. RQ1 asks how Russia links energy coercion, digital manipulation, and climate narratives within hybrid warfare. RQ2 asks through which obstructionist networks those narratives are localized and amplified in Europe. RQ3 asks

when these campaigns weaken support for EU climate securitization and when EU institutions absorb the shock. Together, they make the empirical task clear: to trace how hybrid power becomes cognitive power, and how cognitive power becomes political contestation.

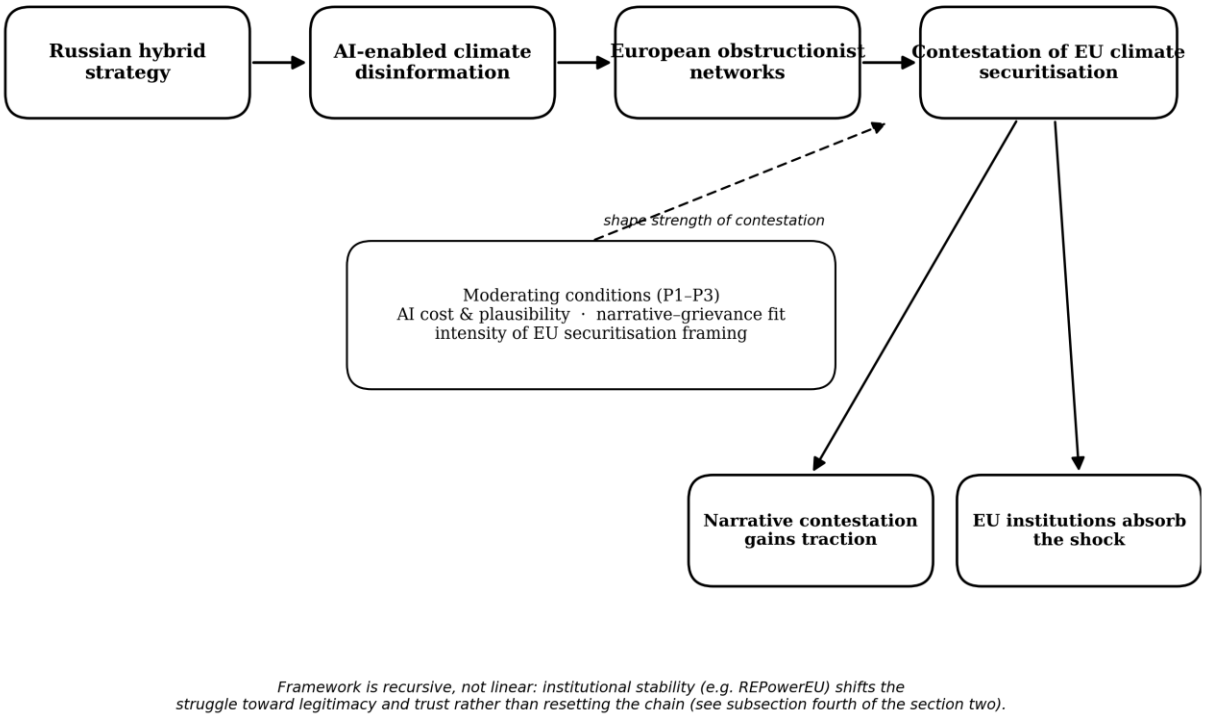

Figure 1: Integrated theoretical framework linking Russian hybrid strategy, climate disinformation, obstructionist networks, and contestation of EU climate securitisation. The figure shows the paper's main theoretical contribution: a conditional model of counter-securitisation, in which contestation gains traction only under specific moderation conditions (Preposition 1–Preposition 3) rather than automatically.

Research Methodology

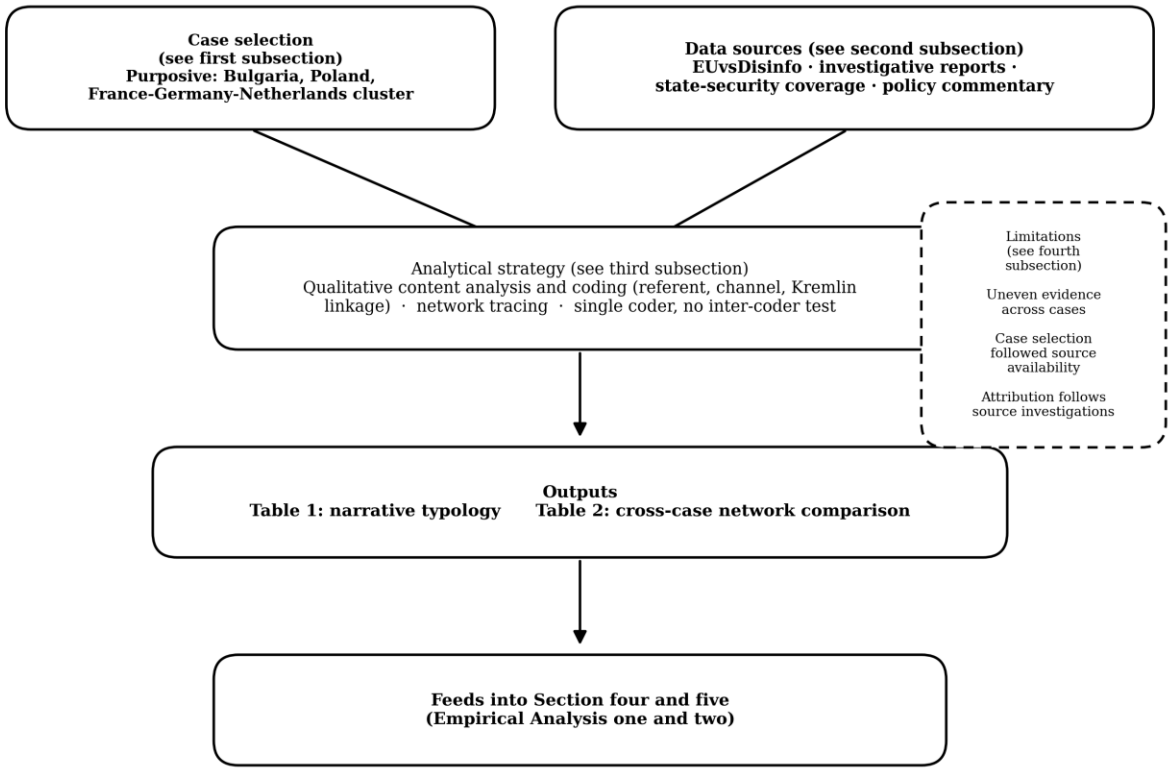

Figure 2: Research design, showing how case selection and data sources feed into the analytical strategy, the resulting outputs (Tables 1 and 2), and the limitations bounding interpretation of the empirical sections.

Case logic

This paper tests the Section 2 framework through purposive, not random, case selection (Yin 2018). Three cases meet the requirement that energy coercion, narrative content, and network amplification trace through one evidentiary base: Bulgaria (Dzhekova et al. 2025), Poland (Grostern 2025), and a linked France-Germany-Netherlands cluster (Logically and EU DisinfoLab 2025). Each rests on a dedicated third-party investigation rather than passing journalistic mention. Czechia appears only in EU-level commentary on Russian nuclear-fuel narratives and is excluded

as a full case, since no dedicated country-level investigation of its disinformation ecosystem was available at the time of writing (De Agostini and Hobhouse 2025). The three cases span the paper's core distinction: Poland shows state-security framing, while Bulgaria and the France-Germany-Netherlands cluster show civil-society and platform-level channels, letting Section 6 compare counter-securitisation across institutional conditions.

Data sources

Four material types inform the analysis. The EUvsDisinfo database (EEAS East StratCom Task Force) is read critically, not as neutral ground truth, and cross-checked against independent reporting. Investigative reports from the Centre for the Study of Democracy (Dzhekova et al. 2025) and Logically and EU DisinfoLab (2025) supply country-level detail. DeSmog's coverage of Poland's counterintelligence commission report supplies a state-security perspective (Grostern 2025). Policy commentary from EUISS, RUSI, and NewClimate Institute situates the cases in the wider literature (De Agostini and Hobhouse 2025; Ince 2025; Jackson et al. 2025). Two EU DisinfoLab platform-policy reports (Romero-Vicente 2023, 2025) inform Section 6.

Analytical strategy

The paper uses qualitative content analysis to identify recurring narrative frames (Krippendorff 2018; Entman 1993), coded by security referent, channel, and stated Kremlin linkage, producing Tables 1 and 2. A single analyst coded the material; no inter-coder reliability test was run, a disclosed constraint. Network tracing follows Starbird et al. (2019), mapping only connections the source investigations already document. Table counts come directly from source reports, not independent platform data. Claude AI Sonnet 5 was used to help draft Figures 1 and 2, but the author reviewed and refined both figures and remains fully responsible for their final form, interpretation, and any revisions.

Limitations

Three limitations follow. The evidence base is uneven: Bulgaria and the France-Germany-Netherlands cluster carry granular, multi-platform documentation, while Poland rests on a single government-linked summary. Attribution to Russian state versus aligned domestic actors follows the source investigations rather than independent verification here. Case selection followed source availability rather than a fixed sampling frame, limiting generalisation, and the evidence base concentrates in 2025-2026 reporting. These constraints match theoretical framework's fourth subsection caution against overclaiming causality and bound interpretation in Conclusion and Policy Implications without limiting the evidence used in emperical section one and two.

Empirical Section one : Russia's Hybrid Climate-Energy Warfare and Contestation of EU Climate Securitization

This section examines how Russian state and state-aligned actors use energy and climate framing to contest EU efforts to treat climate change as a security concern. It draws on three cases with markedly different depths of documentation: Bulgaria, Poland, and a joint France-Germany-Netherlands cluster. Consistent with Section 3, evidence density varies across cases. This asymmetry is flagged explicitly rather than smoothed over.

Russian hybrid energy war narratives targeting Europe and Ukraine

Russia's energy-related hybrid activity against Europe operates on two connected tracks: physical disruption and narrative contestation. On the physical side, Russia has destroyed or occupied roughly half of Ukraine's electricity generation capacity since 2022 (De Agostini and Hobhouse 2025). Its so-called shadow fleet has also been implicated in surveillance near critical

infrastructure, including vessels detained near Finnish and Dutch nuclear and military sites (De Agostini and Hobhouse 2025). These incidents sit alongside a parallel information campaign. When the Baltic states desynchronised from the Russian power grid in February 2025, Kremlin-aligned messaging claimed the move would trigger shortages and price spikes (De Agostini and Hobhouse 2025). Similar narratives followed Poland's and Czechia's efforts to diversify energy supply, framing diversification as economically and environmentally damaging (De Agostini and Hobhouse 2025).

Poland offers the clearest documented case of this narrative-physical pairing. A 2025 review by Poland's military counterintelligence service, covering more than 2,000 documents from 2004 to 2024, concluded that Russia has waged a sustained “cognitive war” against Polish trust in democratic institutions, including NATO and the EU (Grostern 2025). The report identifies bots, trolls, and cyberattacks as delivery mechanisms. One recurring narrative frames the EU’s Emissions Trading Scheme as a scheme by "western bankers" to bankrupt Poland (Grostern 2025). A Polish climate scientist quoted in the same report describes a rise in short-lived fake accounts targeting climate researchers specifically (Grostern 2025). This is one of the few cases in this study where a national intelligence body, rather than a civil-society monitor, attributes disinformation activity directly to Russian state or state-aligned actors.

RUSI analysis raises a more speculative possibility: that Russia could, within the coming decade, experiment with weaponising solar geoengineering technologies to induce climate extremes such as drought or flooding in an adversary state (Ince 2025). No public evidence currently indicates that this has been attempted, or even seriously considered, by Moscow (Ince 2025). This claim is included as a documented expert assessment of future risk, not as an observed event. It should not be read as equivalent to the narrative and infrastructure evidence above.

Climate and Green Deal frames in Kremlin-aligned messaging

Kremlin-aligned outlets have increasingly folded the European Green Deal into broader anti-EU messaging. EUvsDisinfo material documents a shift after the EU's eighteenth sanctions package on Russian oil, when pro-Kremlin channels began framing the Green Deal itself as a hybrid-war target. These channels argue that green energy is a costly scam and that renewable investment is failing (EUvsDisinfo 2025). A 2022 online advertising campaign warned that abandoning Russian gas would bring a new "ice age" to Europe (EUvsDisinfo 2025). In Poland specifically, pro-Kremlin outlets claimed the Green Deal was destroying farming and industry (EUvsDisinfo 2025). The HEAT project's monitoring of France, Germany, and the Netherlands identifies four recurring narrative pillars: a conspiracy milieu, culture-war and partisan discourse, hostile-state-actor content, and messaging aligned with fossil fuel interests (Logically and EU DisinfoLab 2025). Across all three countries, narratives framing climate action as authoritarian or elitist have become more prominent than outright denial of climate science (Logically and EU DisinfoLab 2025). In Bulgaria, the Green Deal and climate change were the second most covered disinformation topic in 2024, generating roughly 40,000 articles. Most portrayed the policy as an instrument of economic destruction (Dzhekova et al. 2025). Telegram amplification in Bulgaria concentrated in a small number of channels, several linked to pro-Kremlin political actors, including the paramilitary-linked "Vasil Levski" network (Dzhekova et al. 2025).

At the EU's external edge, similar framing appears in messaging aimed at partner countries. NewClimate Institute documents a narrative describing EU climate policy as "Western imperialism," targeted particularly at African audiences and framed around resistance to

industrialisation (Jackson et al. 2025). This suggests Russian climate-energy messaging operates on two registers at once: economic self-harm framing for EU domestic audiences, and anti-colonial framing for the EU's partners.

AI-enabled amplification

Evidence for AI-enabled amplification is uneven across cases, and this subsection reports only what is directly documented. At the general level, Stockholm Resilience Centre researchers argue that generative AI, opaque recommender systems, and social bots together create conditions for a "perfect storm" of climate misinformation (Galaz et al. 2023). This is a mechanism-level claim, not a verified case, and it should be read as such.

Case-specific evidence exists for the France-Germany-Netherlands cluster. The HEAT investigation identified one confirmed coordinated inauthentic behaviour network, based in the German-language dataset: ten Facebook profiles created in early-to-mid 2024, three of which used AI-generated images of young women as profile pictures (Logically and EU DisinfoLab 2025). These accounts had modest reach, averaging under 4,000 followers each, and their posts typically drew fewer than a hundred reactions (Logically and EU DisinfoLab 2025). The same investigation traced 404 articles matching climate-disinformation search terms across three Pravda-branded outlets in Germany, France, and the Netherlands, sourced substantially from Russian state media including TASS and RIA Novosti (Logically and EU DisinfoLab 2025). No comparable coordinated network was confirmed in the French or Dutch datasets. Considerable copypasta activity, unattributed reposting of identical text, was nonetheless observed in the French information environment (Logically and EU DisinfoLab 2025).

For Poland, the counterintelligence report documents bots and trolls as delivery mechanisms. It does not attribute this activity specifically to generative AI tools (Grostern 2025). For Bulgaria,

amplification is heavily networked and precisely quantified: nearly 300 Telegram posts on the Green Deal generated over 370,000 views (Dzhekova et al. 2025). The Center for the Study of Democracy (CSD) report does not identify AI-generated content among these mechanisms. Taken together, confirmed generative-AI involvement is currently limited to a small, low-engagement network in one country. Broader claims about AI-driven climate disinformation in this study rest on documented mechanism rather than case-verified scale.

Counter-securitising EU climate security

Read through a securitisation lens, these narratives do more than contest specific policies. They attempt to displace the referent object of EU climate security discourse. The EU frames climate change and energy dependence as threats to citizen welfare and strategic autonomy. Kremlin-aligned messaging instead recasts the EU's own climate policy as the threat, to household budgets, to national sovereignty, and, in messaging aimed at partner countries, to the economic development of the Global South (Jackson et al. 2025; EUvsDisinfo 2025). This is a counter-securitising move. It does not deny that a threat exists; it relocates the threat from Russian energy coercion to the EU's own decarbonisation agenda.

NATO's Strategic Communications Centre of Excellence has tracked a related narrative in Arctic and Nordic-Baltic contexts, in which the West is accused of having invented the climate crisis to justify expanded regional activity (Jackson et al. 2025). Combined with the Poland and Bulgaria findings, this indicates a narrative strategy that adapts to audience. Kremlin-aligned messaging uses economic-harm framing for EU member states directly affected by the green transition, and sovereignty or anti-imperialism framing for the EU's external partners and contested regions. Whether this adaptation reflects centralised strategic coordination or parallel opportunism by loosely affiliated outlets cannot be established from the sources reviewed here.

Table 1: Typology of Russian Climate-Energy Narratives Targeting EU Climate Security

Narrative label	Security referent	Typical communication channels	Documented example	source(s)
Green transition as economic self-harm	Household/economic security	State media, pro-Kremlin news portals, online advertising	2022 “ice age” advertising campaign warning of energy shortages	EUvsDisinfo 2025; De Agostini and Hobhouse 2025
Green Deal as elitist/authoritarian imposition	Political and civil-liberties security	Facebook, X, fringe blogs	German CIB network using AI-generated profile images (2024)	Logically and EU DisinfoLab 2025
Climate policy as cognitive-war target	Institutional/democratic security	State media (Sputnik), bots, trolls, comment sections	Polish counterintelligence findings on the ETS "western bankers" narrative	Grostern 2025
Climate policy as Western imperialism	Geopolitical/developmental security	State-backed media, diplomatic messaging	NATO StratCom COE-monitored Arctic narrative	Jackson et al. 2025
Green Deal as instrument of destruction	National/ethnic security (Bulgaria-specific)	Telegram channels, content aggregators	InfoDefenseBULGARIA and “Vasil Levski” channel networks	Dzhekova et al. 2025

Note: Table 1 summarises five recurring narrative types identified in Kremlin-aligned messaging on EU climate and energy policy. Each row links a narrative to the security referent it targets, its typical communication channel, and one documented example, drawn from the sources cited in Sections four and five.

Emperical Section two: European Obstructionist Networks and AI-Enabled Climate Disinformation

Emperical section one traced how Russian state and state-aligned messaging builds climate-energy narratives that target EU climate security. This section shifts the lens from narrative content to the actors who carry, adapt, and launder these narratives inside EU information ecosystems. It asks which domestic and transnational intermediaries convert Kremlin-aligned framing into locally resonant claims, and what role AI-enabled tools play in that process. As in Section four, evidence density differs sharply across the three cases. That asymmetry is reported as a finding, not facilitated into a uniform claim.

Mapping obstructionist networks

In Bulgaria, amplification concentrates in a small, named set of Telegram channels. InfoDefenseBULGARIA belongs to a documented cluster of more than twenty similarly branded channels operating across most European languages, alongside the paramilitary-linked "Vasil Levski" network already identified in Section 4 and a further channel, Voice of Truth (Dzhekova et al. 2025). The automated content aggregator Novini247 supplements this ecosystem in online media rather than on Telegram (Dzhekova et al. 2025). This is a concentrated structure: few outlets, high reach, and explicit pro-Kremlin alignment among the most-engaged channels.

Poland shows the opposite structure. The counterintelligence commission's review does not identify one dominant channel or platform. It instead describes diffusion across state-linked media such as Sputnik, blogs, and social media comment sections (Grostern 2025). Deputy Prime Minister Krzysztof Gawkowski described the goal as an effort "to create a panic in the infosphere" ahead of Poland's presidential election, and climate scientist Szymon Malinowski reported a rise in short-lived troll accounts attacking researchers directly (Grostern 2025). The network here is diffuse and difficult to isolate, even though the strategic intent behind it is described in strong, explicit terms by Polish officials themselves.

The France-Germany-Netherlands cluster shows a third pattern: a small, technically confirmed core surrounded by wider translation and amplification activity. The HEAT investigation traced a cluster of ten Facebook profiles, deliberately created as personal accounts rather than pages, a format that restricts third-party monitoring (Logically and EU DisinfoLab 2025). Around this core sits a network of Pravda-branded outlets in Germany, France, and the Netherlands. These outlets source content from Russian state media and form part of the wider "Portal Kombat" ecosystem

(Logically and EU DisinfoLab 2025). In France, prominent domestic conspiracists extend this material's reach. Pro-Russia accounts also circulated content invoking German Alternative for Germany (AfD) co-chair Alice Weidel's proposals on carbon taxation. This is an instance of cross-border circulation rather than confirmed coordination with a domestic party (Logically and EU DisinfoLab 2025). Far-right party involvement in this cluster is therefore best read as narrative appropriation by unaffiliated accounts, not as documented party-level coordination.

Localisation of Russian narratives: from hybrid energy war to domestic security frames

Section 2 proposes that narratives travel further where they fit existing domestic grievances. This material allows that proposition to be tested case by case. In Bulgaria, the dominant frame is control rather than cost. InfoDefenseBULGARIA content claims Brussels wants to "control CO2" in order to "control people" (Dzhekova et al. 2025). This is a sovereignty frame, distinct from the economic-destruction framing already reported in empirical section one for the same country.

In Poland, the EUvsDisinfo material used in Section 4 also documents a transnational blame-shift. One Polish outlet attributed paralysing electricity prices to the "self-destructive policy of Brussels and Berlin," folding German energy policy into a domestic grievance about Polish industry (EUvsDisinfo 2025). The frame remains economic, as in empirical section one, but the attributed cause moves outward, from national policy to a combined Brussels-Berlin target.

In the France-Germany-Netherlands cluster, HEAT documents the shift from denial toward elitist framing already noted in emperical section one. Two further, case-specific frames are relevant here. France's Zone a Faibles Emissions (ZFE) low-emission vehicle rules were reframed as targeting ordinary drivers by social class, a claim the investigation's own fact-checkers assessed as inaccurate given exemptions built in for lower-income motorists (Logically and EU DisinfoLab 2025). In the Netherlands, renewable and climate policy was instead framed as an attack on rural

culture, not on national sovereignty (Logically and EU DisinfoLab 2025). Sovereignty, cost, and cultural identity therefore operate as distinct, case-specific entry points into the same underlying contestation of EU climate securitisation.

AI-enabled practices and the contestation of EU climate securitisation

Section four established that confirmed generative-AI involvement is currently limited to the German dataset, where three of the ten HEAT-documented profiles used AI-generated images (Logically and EU DisinfoLab 2025). The point worth developing here is what this means for network capacity, rather than repeating the technical finding. Fabricated personas lower the cost of building an apparently independent, grassroots-looking voice, without requiring a pre-existing partisan base or a genuine online history (Logically and EU DisinfoLab 2025). This capacity effect matters for counter-securitisation more than the modest follower counts suggest, because it allows a small operation to simulate the appearance of organic domestic dissent against EU climate policy.

A second, discursive effect deserves equal weight. Survey research finds that most people already assume AI helps produce and spread false content (García-Faroldi et al. 2025). Where audiences already expect AI involvement, contested claims may gain a plausibility they have not actually earned through verified AI production. This is a distinct mechanism from the production-side "perfect storm" argument already reported in empirical section one (Galaz et al. 2023), and it does not depend on any generative content actually being present. Reporting on declining platform fact-checking commitments compounds this risk, though the precise publication date of that reporting could not be confirmed from the extracted source (Zajmi 2025).

For Bulgaria and Poland, the position established in Section 4 holds without new evidence: neither the CSD report nor the counterintelligence review attributes amplification specifically to generative AI (Dzhekova et al. 2025; Grostern 2025). The regulatory gap underlying all three cases

is structural rather than case-specific. The EU's Digital Services Act does not define coordinated inauthentic behaviour as a systemic-risk category under Articles 34-35 (Logically and EU DisinfoLab 2025). This is consistent with broader findings that EU responses to AI-enabled democratic harm lean on transparency and risk-management tools rather than content removal (Cupac and Sienknecht 2024). It also aligns with the argument that EU digital sovereignty remains constrained by dependence on external technical infrastructure (Calderaro and Blumfelde 2022).

Cross-case comparison: variation in network structure and narrative uptake

Three points of variation stand out. First, network concentration differs by case. Bulgaria's ecosystem is small, named, and high-reach. Poland's is diffuse across state media, blogs, and comment sections. Germany's is smaller still but methodologically confirmed as coordinated; France shows volume and informal signs of coordination without a confirmed network; the Netherlands shows neither a confirmed network nor a comparable volume of activity.

Second, the form of Kremlin attribution differs by case. Bulgaria and Poland rest on institutional attribution: the CSD report names specific channels as pro-Kremlin, and Poland's state commission attributes a "cognitive war" directly to Russian and Belarusian actors (Dzhekova et al. 2025; Grostern 2025). The France-Germany-Netherlands cluster instead rests on content-sourcing analysis, tracing Pravda-branded outlets back to Russian state media, without an equivalent government-commission finding (Logically and EU DisinfoLab 2025). These are different evidentiary strengths, not different degrees of certainty about one underlying claim.

Third, absence of evidence should not be read as absence of activity. The investigators attribute the Netherland's comparatively thin findings to the limited strategic value of targeting a small Dutch-language audience with high English-language proficiency, rather than to any confirmed

absence of exposure (Logically and EU DisinfoLab 2025). This caveat is reported here rather than resolved, consistent with this study's approach to evidentiary gaps elsewhere.

Read against Securitisation Theory, this variation matters because the audience component of the securitising speech act differs by case. Bulgaria and Poland show durable narrative uptake among an identifiable domestic audience. The France-Germany-Netherlands cluster shows more translation and circulation activity than confirmed audience uptake. Obstructionist networks may therefore be entering EU information environments unevenly, reaching susceptible audiences in some member states well before, if ever, they reach a comparable threshold in others.

Table 2: Obstructionist Networks in Selected Member States

Case	Key actors	Dominant narratives	Documented Kremlin links	Evidence of AI-enabled amplification	Source(s)
Bulgaria	Concentrated Telegram cluster (InfoDefenseBULGARIA network, Voice of Truth, Vasil Levski) + automated aggregator Novini247	Sovereignty/control framing ("control CO2 → control people"); EGD as economic destruction	Explicit - channels independently identified as pro-Kremlin	Not documented - automated aggregation only	Dzhekova et al. 2025
Poland	Diffuse: state-linked media, blogs, comment sections; no single dominant outlet	EGD/decarbonisation as threat to farmers and industry; blame-shifted to Brussels-Berlin	Explicit, institutional - state commission attribution	Referenced generically (bots/trolls); no AI-tool attribution	Grostern 2025; EUvsDisinfo 2025
Germany	10-profile Facebook cluster (personal-account format); Pravda DE	Climate policy as elitist/authoritarian overreach	Indirect - traced via Pravda/Portal Kombat sourcing	Documented - 3 of 10 profiles used AI-generated images	Logically and EU DisinfoLab 2025
France	Pravda Français; domestic conspiracist amplifiers; Telegram channels with informal coordination signs	ZFE rules reframed as class-targeted; elite-control framing	Indirect -Pravda Français sourced from Russian state media	Not confirmed-copypasta activity only, no confirmed CIB	Logically and EU DisinfoLab 2025
Netherlands	Pravda Nederland; limited domestic amplifier base	Climate/renewable policy as attack on rural culture	Circumstantial-republishing only, no confirmed network	Not documented	Logically and EU DisinfoLab 2025

Note: Table 2 compares obstructionist networks across the five country cases. It sets out the key actors, dominant narratives, and documented Kremlin links for each case, alongside the evidence available for AI-enabled amplification. Evidence density varies by case, and this variation is reported directly rather than smoothed into a uniform claim.

Discussion and Theoretical Implications

Securitization and Counter-Securitization

Sections four and five confirm the referent-object displacement introduced in subsection fourth of the section four: Russian-aligned and obstructionist narratives recast EU climate policy itself as the threat, not the underlying climate risk (Jackson et al. 2025; EUvsDisinfo 2025). This is consistent with the Copenhagen School's core claim that security is constituted through a speech act rather than an objective condition (Baele and Jalea 2023). The empirical variation documented in empirical Section two nonetheless exposes a limitation in the theory as usually applied. Bulgaria and Poland show durable narrative uptake among an identifiable domestic audience, while the France-Germany-Netherlands cluster shows more circulation than confirmed uptake. Securitization theory offers detailed guidance on audience acceptance of an original securitising move (Rhinard et al. 2023; Morsut and Rhinard 2025), but it says less about when a counter-securitising move succeeds with an audience. The present evidence suggests that success is uneven and audience-dependent rather than automatic. Warner and Boas's (2019) warning that securitising climate policy can backfire finds no confirmed instance either way in this dataset. No case demonstrates that EU climate securitisation has been discredited by contestation, and none shows the contestation itself backfiring on its proponents. This is an evidentiary limit rather than a theoretical failure, and it counsels caution before generalising about counter-securitisation's effectiveness.

Hybrid and Cognitive Warfare in the Energy-Resources-Climate Nexus

Emperical section one documents Russian hybrid activity operating on two connected tracks: physical disruption and narrative contestation, extending Geri’s (2024) argument that Russian hybrid warfare now reaches the energy-resources-climate nexus. The AI-enabled dimension calls

for caution, however. As subsection third of the empirical section two, develops, confirmed generative-AI involvement remains limited to one small network. Its main effect currently operates through the discursive plausibility mechanism established there (García-Faroldi et al. 2025), rather than through production scale (Galaz et al. 2023). Existing hybrid and cognitive warfare frameworks do not clearly separate this distinction (Kalniete and Pildegovics 2021; Bazarkina 2022).

Obstructionist Networks as a Theoretical Category

Subsection fourth of the empirical section two, documents three structurally distinct obstructionist configurations: Bulgaria's concentrated cluster, Poland's diffuse ecosystem, and Germany's smaller but confirmed network. This German network sits within a wider Pravda-branded ecosystem across the France-Germany-Netherlands cluster (Dzhekova et al. 2025; Grostern 2025; Logically and EU DisinfoLab 2025). This variation suggests that "obstructionist network" should not be treated as a single, monolithic category of intermediary, as hybrid warfare literature sometimes implies when describing proxy or amplifier actors (Kalniete and Pildegovics 2021). The cases instead suggest a spectrum, running from concentrated and institutionally attributable structures to diffuse and only indirectly attributable ones. Starbird et al. (2019) framing of disinformation as collaborative work, rather than centrally directed propaganda, helps explain this variation. Obstructionist actors in Bulgaria and Poland appear to adapt Kremlin-aligned narratives to local grievances rather than simply relaying them, while the French and Dutch cases show narrative appropriation by unaffiliated accounts rather than confirmed party-level coordination. This distinction carries theoretical weight. Network structure appears to shape not only reach but also the kind of evidentiary claim a researcher can make about Kremlin linkage, from explicit institutional attribution to inference from content-sourcing analysis alone. Treating obstructionist

networks as a differentiated category, rather than a uniform proxy actor, adds analytical precision that existing hybrid warfare frameworks have not fully developed.

Refining the Integrated Framework

Taken together, these findings support a refinement of the integrated framework proposed in subsection fourth of the theoretical framework, rather than its wholesale revision. The propositions linking Russian hybrid strategy, AI-enabled disinformation, obstructionist networks, and counter-securitisation are broadly consistent with the empirical record. The record also specifies conditions under which this chain plausibly operates. Three boundary conditions emerge. First, narrative uptake appears conditional on pre-existing domestic grievance fit. Cases with strong grievance alignment, such as Poland and Bulgaria, show durable institutional attribution and audience uptake, while the France-Germany-Netherlands cluster shows weaker uptake despite comparable narrative circulation. Second, the strength of Kremlin attribution varies by evidentiary tier, from direct government-commission findings to inference from content-sourcing analysis, and this variation should condition how confidently any single case is generalised. Third, AI's contribution currently appears more discursive than productive. It shapes audience expectations about the credibility of information more than it currently demonstrates capacity to manufacture disinformation at scale. This paper's original theoretical contribution is therefore a conditional model of AI-enabled counter-securitisation, one that specifies when the mechanism plausibly operates rather than asserting that it operates uniformly. This is a modest but necessary corrective to hybrid warfare and securitization literatures that have not yet been tested systematically against country-level variation in evidentiary depth (Baele and Jalea 2023; Libiseller 2023). The following section draws out what this conditional model implies for EU policy responses and for the limitations of the present study.

Conclusion and Policy Implications

This paper has argued that AI-enabled climate disinformation functions as a form of counter-securitisation within the energy-resources-climate nexus, rather than as a simple denial of climate science (Geri 2024; Morsut and Rhinard 2025). Russian-aligned and obstructionist actors do not reject the existence of climate change. They contest who defines the threat and which institutions may act on it, recasting EU decarbonisation itself as the source of insecurity (Morsut and Rhinard 2025). The empirical record supports a conditional rather than a uniform model of this mechanism. AI's contribution currently operates more through a discursive plausibility effect than through demonstrated production capacity (Galaz et al. 2023).

The empirical sections identified a dual-track Russian strategy combining physical disruption of energy infrastructure with narrative contestation of the green transition (De Agostini and Hobhouse 2025). Obstructionist networks varied structurally across cases. Bulgaria showed a concentrated, named Telegram cluster; Poland a diffuse, state-linked ecosystem; the France-Germany-Netherlands cluster a smaller but methodologically confirmed coordinated network (Dzhekova et al. 2025; Grostern 2025; Logically and EU DisinfoLab 2025). Confirmed generative-AI involvement remained limited to this last case.

These findings carry several policy implications for the European Union. Strategic pre-bunking and sustained public communication on energy and climate policy may help pre-empt the narrative contestation documented here (De Agostini and Hobhouse 2025). Fact-checking networks such as the European Digital Media Observatory, alongside the EEAS's FIMI mandate and the EUvsDisinfo platform, already provide institutional infrastructure for this task (Jackson et al.

2025; NewClimate Institute 2026). Their reach beyond domestic audiences, however, remains uneven. On AI governance, the Digital Services Act does not currently classify coordinated inauthentic behaviour as a systemic risk under Articles 34–35 (Logically and EU DisinfoLab 2025). This leaves a structural gap that transparency and risk-management measures alone may not close (Cupac and Sienknecht 2024). Coordination among Member States also remains limited, as ministers themselves acknowledged when discussing the absence of effective countermeasures (Hodgson 2025).

Several limitations qualify these conclusions. Attribution rests on uneven evidentiary tiers, from direct government-commission findings to inference from content-sourcing analysis alone, and this variation should temper cross-case generalisation. The geographic scope is limited to three cases and four countries, and securitization theory itself remains under-tested against this kind of country-level variation (Baele and Jalea 2023). Future research should extend the comparative base and examine how counter-securitising narratives interact with audience uptake over time.

References

Baele, Stephane J., and Diana Jalea. 2023. "Twenty-Five Years of Securitization Theory: A Corpus-Based Review." *Political Studies Review* 21 (2): 376–389. https://doi.org/10.1177/14789299211069499.

Bajarunas, Eitvydas. 2020. "Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond." *European View* 19 (1): 62–70. https://doi.org/10.1177/1781685820912041.

Bazarkina, Darya Yu. 2022. "Countermeasures for Hybrid Threats: The Experience of the European Union and Its Member States." *Herald of the Russian Academy of Sciences 92* (Suppl. 4): S315–S320. https://doi.org/10.1134/S1019331622100033.

Briggs, Chad M. 2020. "Climate Change and Hybrid Warfare Strategies." *Journal of Strategic Security* 13 (4): 45–57. https://doi.org/10.5038/1944-0472.13.4.1864.

Briggs, Chad M., and Miriam Matejova. 2023. "Hybrid Warfare in Ukraine and Its Impact on Climate Politics." *Czech Journal of International Relations* 58 (2). https://doi.org/10.32422/cjir.745.

Calderaro, Andrea, and Stella Blumfelde. 2022. "Artificial Intelligence and EU Security: The False Promise of Digital Sovereignty." *European Security* 31 (3): 415–434. https://doi.org/10.1080/09662839.2022.2101885.

Cupac, Jelena, and Mitja Sienknecht. 2024. "Regulate Against the Machine: How the EU Mitigates AI Harm to Democracy." *Democratization 31* (5): 1067–1090. https://doi.org/10.1080/13510347.2024.2353706.

De Agostini, Leonardo, and Caspar Hobhouse. 2025. "Fuel, Fear and Falsehoods: Defending Europe and Ukraine from Russia's Hybrid Energy War." *European Union Institute for Security Studies*, Commentary, December 10. Fuel, fear and falsehoods: Defending

Europe and Ukraine from Russia's hybrid energy war | European Union Institute for Security Studies.

Dreyer, Marius, and Bente Holm. 2025. "Transformative Securitization: Rethinking the Copenhagen School in Light of COVID-19, Climate Change, and the War in Ukraine." *Cooperation and Conflict* 60 (4): 1028–1053. https://doi.org/10.1177/00108367251382793.

Dzhekova, Rositsa, Goran Georgiev, Elizaveta Polyakova, and Deyan Petrov. 2025. *Distorted Realities: Exposing Malign Influence in Bulgarian Online Discourse.* Sofia: Center for the Study of Democracy. Distorted Realities: Exposing Malign Influence in Bulgarian Online Discourse. Country Report - BROD.

Entman, Robert M. 1993. "Framing: Toward Clarification of a Fractured Paradigm." *Journal of Communication* 43 (4): 51–58. 10.1111/j.1460-2466.1993.tb01304.x.

EUvsDisinfo. 2025. "Weaponising Climate Change to Undermine the West." EUvsDisinfo. https://euvsdisinfo.eu/weaponising-climate-change-to-undermine-the-west/.

Galaz, Victor, Hannah Metzler, Stefan Daume, Andreas Olsson, Björn Lindström, and Arvid Marklund. 2023. *Climate Misinformation in a Climate of Misinformation*. Research brief. Stockholm: Stockholm Resilience Centre and Beijer Institute of Ecological Economics. https://www.stockholmresilience.org/research/synthesis-reports/climate-misinformation.html.

García-Faroldi, Livia, Laura Teruel, and Sonia Blanco. 2025. "Unmasking AI's Role in the Age of Disinformation: Friend or Foe?" *Journalism and Media* 6 (1): 19. https://doi.org/10.3390/journalmedia6010019.

Geri, Maurizio. 2024. "Understanding Russian Hybrid Warfare against Europe in the Energy Sector and in the Future Energy-Resources-Climate Security Nexus." *Journal of Strategic Security* 17 (3): 15–34. https://doi.org/10.5038/1944-0472.17.3.2270.

Grostern, Joey. 2025. "Russia 'Spread Conspiracy Theories and Attacked Climate Scientists in Poland.'" DeSmog, February 3. https://www.desmog.com/2025/02/03/russia-spread-conspiracy-theories-and-attacked-climate-scientists-in-poland/.

Hodgson, Robert. 2025. "EU Governments Discuss Action on Disinformation over Climate Policy." Euronews, April 29. https://www.euronews.com/my-europe/2025/04/29/eu-governments-discuss-action-on-disinformation-over-climate-policy.

Hoeffler, Catherine, Stéphanie C. Hofmann, and Frédéric Mérand. 2024. "The Polycrisis and EU Security and Defence Competences." *Journal of European Public Policy* 31 (10): 3224–48. https://doi.org/10.1080/13501763.2024.2362762.

Hoffman, Frank G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Iampolsca, Daniela. 2026. "From Trolls to Generative AI: Russia's Disinformation Evolution." Policy Brief No. 227. Waterloo, ON: Centre for International Governance Innovation, February. https://www.cigionline.org/publications/from-trolls-to-generative-ai-russias-disinformation-evolution/.

Ince, Matt. 2025. "Unnatural Disasters: The Next Front in Russia's Hybrid War." RUSI Commentary, July 14. https://www.rusi.org/explore-our-research/publications/commentary/unnatural-disasters-next-front-russias-hybrid-war.

Jackson, Sarah, Ines Paiva, and Imogen Outlaw. 2025. *Understanding the Global Climate Disinformation Landscape and Strengthening the EU's Response*. Briefing. Cologne: NewClimate Institute. https://newclimate.org/sites/default/files/2025-12/newclimate-briefing-climate-disinformation-decem25.pdf.

Kalniete, Sandra, and Tomass Pildegovics. 2021. "Strengthening the EU's Resilience to Hybrid Threats." *European View* 20 (1): 23–33. https://doi.org/10.1177/17816858211004648.

Krippendorff, Klaus. *Content Analysis: An Introduction to Its Methodology*. Fourth Edition,Thousand Oaks, CA: SAGE Publications, Inc., 2019. https://doi.org/10.4135/9781071878781.

Liberatore, Angela. 2013. "Climate Change, Security and Peace: The Role of the European Union." *Review of European Studies* 5 (3): 83-94.10.5539/res.v5n3p83.

Libiseller, Chiara. 2023. "Hybrid Warfare as an Academic Fashion." *Journal of Strategic Studies* 46 (4): 858–880. https://doi.org/10.1080/01402390.2023.2177987.

Logically and EU DisinfoLab. 2025. *HEAT: Harmful Environmental Agendas and Tactics: A Look at France, Germany, and the Netherlands*. June 2025. https://www.disinfo.eu/wp-content/uploads/2025/06/20250623-heat-harmful-environmental-agendas-tactics.pdf.

Mees, Heleen, and Jana Surian. 2023. "Dutch National Climate Change Adaptation Policy through a Securitization Lens: Variations of Securitization." *Frontiers in Climate* 5: 1080754. doi: 10.3389/fclim.2023.1080754.

Morsut, Claudia, and Mark Rhinard. "The Collective Securitisation of Climate Change: Implications for Climate Adaptation Policy in the United Nations and European Union." *Review of International Studies*, 2025, 1–26. https://doi.org/10.1017/S0260210525100867.

NewClimate Institute. 2026. "How Climate Disinformation Is Reshaping Geopolitics – and Europe's Role in Fighting It." NewClimate Institute Blog, January 12. https://newclimate.org/news/how-climate-disinformation-is-reshaping-geopolitics-and-europes-role-in-fighting-it.

Rhinard, Mark, Claudia Morsut, Elisabeth Angell, et al. 2023. "Understanding Variation in National Climate Change Adaptation: Securitization in Focus." *Politics and Space* 42 (4): 676–696. https://doi.org/10.1177/23996544231212730.

Romero-Vicente, Ana. 2023. "Don't Stop Me Now: The Growing Disinformation Threat Against Climate Change." EU DisinfoLab, February 6. https://www.disinfo.eu/publications/dont-stop-me-now-the-growing-disinformation-threat-against-climate-change/.

Romero-Vicente, Ana. 2025. "Platforms' Policies on Climate Change Misinformation." EU DisinfoLab, July. https://www.disinfo.eu/wp-content/uploads/2025/07/20250722-platforms-policies-on-climate-change-misinformation.pdf.

Starbird, Kate, Ahmer Arif, and Tom Wilson. 2019. "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations." *Proceedings of the ACM on Human-Computer Interaction* 3: 1–26. https://doi.org/10.1145/3359229.

Warner, Jeroen, and Ingrid Boas. 2019. "Securitization of Climate Change: How Invoking Global Dangers for Instrumental Ends Can Backfire." *Environment and Planning C: Politics and Space* 37 (8): 1471–1488. DOI: 10.1177/2399654419834018.

Wendler, Frank. 2023. "The European Green Deal Agenda After the Attack on Ukraine: Exogenous Shock Meets Policy-Making Stability." *Politics and Governance* 11 (4): 352–364. The European Green Deal Agenda After the Attack on Ukraine: Exogenous Shock Meets Policy-Making Stability | Article | Politics and Governance.

Yin, Robert K. 2018. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks, CA: Sage.

Zajmi, Xhoi. 2025. "Fake Climate News Thriving as Politics and AI Turbocharge Disinformation Crisis." Euractiv, February 12. https://www.euractiv.com/section/tech/news/fake-climate-news-thriving-as-politics-and-ai-turbocharge-disinformation-crisis/.

[i] Abhinay Rai is a PhD Scholar, Department of Political Science, Guru Ghasidas Vishwavidyalaya (Central University, NAAC A++), Bilaspur, Chhattisgarh, India.

[ii] Dr. Ram Babu is Assistant Professor, Department of Political Science, Guru Ghasidas Vishwavidyalaya (Central University, NAAC A++), Bilaspur, Chhattisgarh, India.

[iii] Rahul Kumar Tiwari is a PhD Scholar, Department of Political Science, Guru Ghasidas Vishwavidyalaya (Central University, NAAC A++), Bilaspur, Chhattisgarh, India.