International Journal of Social Sciences

Caucasus International University
Volume 6, Issue 3

Journal homepage: http://journal.ciu.edu.ge/

DOI: https://doi.org/10.55367/ILYI5249



*Conference proceedings – **International scientific conference "Contemporary Challenges in International Relations, International Law and Media"** organised by Caucasus International University*
Held on March 12-13, 2026 in Tbilisi

Europe's Tripwire: Cables, Courts, and Feeds in Russia's Hybrid Offensive

Irina Tsukerman [a1]

[a] Juris Doctor, Fordham University School of Law, United States
President of Scarab Rising, Inc.

ARTICLE INFO ABSTRACT

Keywords:

Hybrid threats

Lawfare

Critical infrastructure resilience

Disinformation ecosystems

Black Sea region

Introduction. Europe is increasingly exposed to synchronised hybrid campaigns in which physical disruption, legal pressure, and information manipulation operate as an integrated system. While existing research has examined critical infrastructure interference, lawfare, and disinformation as distinct phenomena, less attention has been paid to how these domains are deliberately coordinated in time and effect. This article situates the problem within the broader scholarship on hybrid coercion and addresses the gap concerning cross-domain synchronisation and its cumulative impact on governance, economic stability, and public compliance.

Materials and Methods. The study employs a qualitative, cross-domain analytical approach. It maps incidents involving seabed cable interference, rail and electricity-grid disruption, GPS spoofing, and territorial borderisation alongside patterns of strategic litigation in investment arbitration, maritime disputes, human rights forums, and challenges to sanctions regimes. This mapping is combined with structured analysis of information operations across digital platforms and broadcast ecosystems, with particular attention to activity during periods of energy stress or extreme weather. Georgia is examined as a forward case to trace early pattern formation and westward diffusion. In addition, the article integrates China into the analytical framework as a strategic enabler rather than a direct operational actor. It examines how Chinese-linked narratives, economic relationships, technological dependencies, and diplomatic positioning interact with Russian coercive activity to shape European institutional responses.

[1] Corresponding author.
E-mail addresses: itsukerman@itsukermanatlaw.com (I. Tsukerman).
ORCID: https://orcid.org/0009-0004-9118-2600

Received: 12/04/2026 Revised: 30/06/2026 Accepted: 20/07/2026 Published: 26/11/2026
E-ISSN 2720-8036 / © 2026 The Author(s). Published in The International Journal of Social Sciences by Caucasus International University.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

Results. The analysis demonstrates that physical interference, litigation activity, and information operations are frequently synchronised rather than episodic. These actions reinforce one another by amplifying uncertainty, administrative burden, and institutional hesitation. The compound effects observed include increased insurance premia, procurement delays, regulatory risk aversion, and declining public compliance during crises, even in the absence of overt military escalation.

Conclusions. The article concludes that effective deterrence in this environment depends on transforming legal and regulatory frameworks into operational instruments. It proposes a legal-operational playbook that links rapid forensics and joint attribution to response thresholds, enhanced transparency, crisis communications, and the targeting of intermediary enablers. Georgia emerges as an early-warning flank whose experience highlights how deterrence can be rendered auditable and procedural rather than declaratory. By distinguishing between operational authorship and strategic enablement, the study demonstrates how external actors can reinforce hybrid coercion indirectly through narrative convergence, sanctions mitigation, and otherwise by creating dependencies that make targeted states more vulnerable.

ევროპის სასიგნალო ზღვარი: კაბელები, სასამართლოები და საინფორმაციო ნაკადები რუსეთის ჰიბრიდულ შეტევაში

ირინა ცუკერმანი [a] [2]

[a] სამართლის დოქტორი, ფორდჰემის უნივერსიტეტის სამართლის სკოლა, აშშ
Scarab Rising, Inc.-ის პრეზიდენტი

სტატიის შესახებ

საკვანძო სიტყვები:

ჰიბრიდული საფრთხეები

სამართლებრივი ომი

კრიტიკული ინფრასტრუქტურის მდგრადობა

დეზინფორმაციული ეკოსისტემები

შავი ზღვის რეგიონი

აბსტრაქტი

ევროპა სულ უფრო მეტად ექცევა სინქრონიზებული ჰიბრიდული კამპანიების ზემოქმედების ქვეშ, რომლებშიც ფიზიკური დივერსია, სამართლებრივი ზეწოლა და საინფორმაციო მანიპულაცია ერთიანი სისტემის სახით მოქმედებს. არსებული კვლევები კრიტიკული ინფრასტრუქტურის ფუნქციონირებაში ჩარევას, სამართლებრივი მექანიზმების ბოროტად გამოყენებასა და დეზინფორმაციას ძირითადად ცალკეულ მოვლენებად განიხილავს, თუმცა ნაკლები ყურადღება ეთმობა იმას, თუ როგორ ხდება ამ სფეროების მიზანმიმართული კოორდინაცია დროისა და მიღწეული ეფექტის მიხედვით. წინამდებარე სტატია ამ პრობლემას ჰიბრიდული იძულების შესახებ არსებული ფართო სამეცნიერო ლიტერატურის კონტექსტში განიხილავს და ყურადღებას ამახვილებს კვლევით ხარვეზზე, რომელიც უკავშირდება სხვადასხვა სფეროს შორის სინქრონიზაციასა და მის კუმულაციურ გავლენას მმართველობაზე, ეკონომიკურ სტაბილურობასა და საზოგადოების მიერ წესებისა და ინსტიტუციური მოთხოვნების დაცვაზე.

მასალები და მეთოდები. კვლევა იყენებს თვისებრივ, სფეროთაშორის ანალიტიკურ მიდგომას. იგი სისტემურად აჯგუფებს და აანალიზებს ზღვის ფსკერზე განთავსებული კაბელების ფუნქციონირებაში ჩარევის, სარკინიგზო და ელექტროენერგეტიკული ქსელების შეფერხების, GPS სიგნალების გაყალბებისა და ტერიტორიების „ბორდერიზაციის“ შემთხვევებს, აგრეთვე სტრატეგიული სამართალწარმოების პრაქტიკას საინვესტიციო არბიტრაჟში, საზღვაო დავებში, ადამიანის უფლებათა დაცვის ფორუმებსა და სანქციების რეჟიმების გასაჩივრების პროცესებში. აღნიშნული მონაცემების შეჯერება ხდება ციფრულ პლატფორმებსა და სამაუწყებლო საინფორმაციო სივრცეში წარმოებული საინფორმაციო ოპერაციების სტრუქტურირებულ ანალიზთან, განსაკუთრებული ყურადღებით ენერგეტიკული კრიზისებისა და ექსტრემალური ამინდის პერიოდებზე. საქართველო განხილულია, როგორც მოწინავე შემთხვევა, რომელიც ადრეული მოდელების ფორმირებისა და მათი დასავლეთის მიმართულებით გავრცელების მიკვლევის შესაძლებლობას

[2] ავტორი კორესპონდენტი.
ელექტრონული ფოსტა: itsukerman@itsukermanatlaw.com (ი.ცუკერმანი).
ORCID: https://orcid.org/0009-0004-9118-2600

იძლევა. სტატია ანალიტიკურ ჩარჩოში ჩინეთსაც აერთიანებს, როგორც სტრატეგიულ ხელშემწყობ აქტორს და არა უშუალო ოპერატიულ მონაწილეს. კვლევა განიხილავს, თუ როგორ ურთიერთქმედებს ჩინეთთან დაკავშირებული ნარატივები, ეკონომიკური ურთიერთობები, ტექნოლოგიური დამოკიდებულებები და დიპლომატიური პოზიციონირება რუსეთის იძულებით მოქმედებებთან და როგორ ზემოქმედებს ეს ურთიერთქმედება ევროპული ინსტიტუტების რეაგირებაზე.

შედეგები. ანალიზი აჩვენებს, რომ ფიზიკური ჩარევა, სამართალწარმოებასთან დაკავშირებული აქტივობა და საინფორმაციო ოპერაციები ხშირად სინქრონიზებულად ხორციელდება და არა ცალკეული, ეპიზოდური მოქმედებების სახით. ეს მოქმედებები ერთმანეთს აძლიერებს გაურკვევლობის ზრდის, ადმინისტრაციული დატვირთვისა და ინსტიტუციური ყოყმანის გაძლიერების გზით. გამოვლენილი კომპლექსური შედეგები მოიცავს სადაზღვევო პრემიების ზრდას, შესყიდვების შეფერხებას, რეგულაციებთან დაკავშირებული რისკების მიმართ ინსტიტუციური სიფრთხილის ზრდასა და კრიზისების დროს საზოგადოების მიერ წესებისა და ინსტიტუციური მოთხოვნების დაცვის შემცირებას, მათ შორის ღია სამხედრო ესკალაციის გარეშეც.

დასკვნები. სტატიის თანახმად, ასეთ გარემოში ეფექტიანი შეკავება დამოკიდებულია სამართლებრივი და მარეგულირებელი ჩარჩოების ოპერატიულ ინსტრუმენტებად გარდაქმნაზე. კვლევა გვთავაზობს სამართლებრივ-ოპერატიულ სამოქმედო მოდელს, რომელიც სწრაფ ექსპერტიზასა და ერთობლივ ატრიბუციას აკავშირებს რეაგირების ზღვრებთან, გამჭვირვალობის გაძლიერებასთან, კრიზისულ კომუნიკაციებთან და შუამავალი ხელშემწყობი აქტორების წინააღმდეგ მიზანმიმართულ ზომებთან. საქართველო წარმოჩნდება ადრეული გაფრთხილების ფლანგად, რომლის გამოცდილებაც აჩვენებს, თუ როგორ შეიძლება შეკავება გახდეს შემოწმებადი და პროცედურულად განსაზღვრული და არა მხოლოდ დეკლარაციული. ოპერატიული ავტორობისა და სტრატეგიული ხელშეწყობის ერთმანეთისგან გამიჯვნით, კვლევა აჩვენებს, თუ როგორ შეუძლიათ გარე აქტორებს ჰიბრიდული იძულების ირიბად გაძლიერება ნარატივების თანხვედრის, სანქციების შედეგების შერბილების ხელშეწყობისა და ისეთი დამოკიდებულებების შექმნის გზით, რომლებიც სამიზნე სახელმწიფოების მოწყვლადობას ზრდის.

ევროპის საგანგაშო ზღვარი: კაბელები, სასამართლოები და საინფორმაციო არხები რუსეთის ჰიბრიდულ შეტევაში.

1. Introduction

Europe is confronting a phase shift in hybrid coercion in which physical disruption, legal pressure, and information manipulation function as mutually reinforcing systems rather than parallel lines of effort. Adversaries are operating just below the threshold of armed conflict, exploiting ambiguity to constrain responses and avoid escalation. Interference with critical infrastructure, legal manoeuvring, and coordinated influence operations during moments of heightened societal stress can nevertheless become matters of strategic significance.

The central research question addressed in this article concerns how these domains are deliberately synchronised and why their interaction produces effects that exceed the impact of any single instrument. Existing scholarship has established hybrid warfare, lawfare, and disinformation as recognised tools of state competition, but it has largely examined them in isolation. While definitions of hybrid warfare frequently describe it as playing out at all levels (strategic, operational, tactical), much analysis neglects the legal and regulatory dimension. This compartmentalisation has limited understanding of how physical, legal, and informational pressures interact in practice.

More recent work has begun to challenge this separation. Michael Kofman, Anya Fink, and Jeffrey Edmonds observe that Russian operations frequently exhibit “calibrated escalation,” suggesting intentional sequencing, not only opportunistic overlap (Kofman, Fink, and Edmonds, 2020). Andrew Monaghan similarly argues that ambiguity functions as a method for constraining Western decision-making by exploiting biases for legal and political caution (Monaghan, 2019). By contrast, Alexander Lanoszka cautions that not all activity below the threshold should be assumed to reflect coherent orchestration, warning that hybrid warfare risks becoming an analytically overstretched concept (Lanoszka, 2016). This disagreement over design versus improvisation remains unresolved in the literature.

Legal scholarship introduces an additional dimension, emphasising how the legal process itself can serve as a coercive instrument. Parallel research on information operations highlights institutional effects rather than persuasion as the primary outcome. W. Lance Bennett and Steven Livingston describe a “disinformation order” in which the erosion of trust and authority weakens the capacity for governance during crises (Bennett & Livingston, 2018). These insights suggest that legal and informational tools may be most effective when aligned with physical disruption.

This article advances the argument that strategic innovation lies in the deliberate timing and sequencing of actions across these domains. It situates the analysis within the European security environment while treating Georgia as an early-warning flank where techniques are tested and later observed migrating westward. The purpose of this research is to map a synchronised hybrid system and to demonstrate how deterrence can be translated from declaratory policy into auditable legal and regulatory procedures. The main conclusion is that resilience depends less on new doctrine than on the operationalisation of existing tools in a coordinated and time-bound manner.

2. Literature Review

The contemporary literature on hybrid conflict in Europe is anchored in the recognition that coercion increasingly operates below the threshold of provoking armed conflict and is designed to push the envelope while constraining responses. Frank G. Hoffman characterises hybrid warfare as "the blurring of modes of war, the blurring of who fights, and what technologies are brought to bear," and he frames it as a purposeful combination of "conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder" (Hoffman, 2007). Ofer Fridman compares Hoffman's conception of hybrid war with Russia's gibridnaya voyna, a direct translation but more akin to subversive-war, finding that the Russian concept has "very little in common with the Western, very military-oriented understanding" because of "intentional inaccuracy introduced for political reasons" rather than a "methodological misunderstanding" (Fridman, 2017). Alexander Lanoszka advances a corrective to overexpansive usage by arguing for a more limited definition: "in which an aggressor uses the social links — that is, ethnic ties — it has with a target society to subvert it under the shadow of military power. The hybridity of the strategy comes from combining the actual use of guerrilla tactics and other forms of subversion — be they sabotage, criminal disorder and agitation — with the threat of escalation in the conventional military domain." In other words, many Russian malign activities labelled as hybrid war are, he argues, better understood as what they are: "Electoral interference is simply electoral interference. Killing a former spy abroad is extraterritorial (and extrajudicial) murder." (Lanoszka, 2018). Mark Galeotti makes a parallel methodological warning, describing the hybrid label as at risk of becoming a catch-all term that can lose explanatory value (Galeotti, 2016). Nevertheless, the dizzying array of means employed under a cloak of official ambiguity is precisely the point. In the case of Russia, the danger is in emphasizing the first word ("hybrid") in a way that modifies, if not negates, the second ("war "). For the Kremlin, electoral interference, extrajudicial killings, weaponized migration, co-opting or covertly using influencers, and other hybrid actions fall under their forever war on the American-led, rules-based international order (Eggen, 2025; U.S. Department of Justice, 2024). Russia's redefinition of red lines and ability to avoid responsibility for acts of war, including violations of airspace and even the debilitating if not deadly targeting of American diplomats and intelligence officers, is a testament to the deflective power of hyping "hybrid" and has helped pave the way for ever-increasing overt aggressive actions all the way up to the full-scale invasion of Ukraine (Weiss et al., 2024).

A second strand of the literature concentrates on whether hybrid coercion is best understood as coherent orchestration or adaptive opportunism. Michael Kofman, Anya Fink, and Jeffrey Edmonds argue that Russian practice frequently reflects "calibrated escalation," suggesting intentionality in how pressure is raised while remaining beneath conventional thresholds (Kofman et al., 2020). Andrew Monaghan reinforces this interpretation by treating ambiguity as a method rather than a by-product, and by emphasising how strategic effects can be achieved through administrative friction and decision delay rather than outright confrontation (Monaghan, 2019). Forrest Morgan and colleagues, writing on grey-zone competition, highlight how uncertainty over attribution and intent is a mechanism for slowing counteraction as well as fracturing consensus (Morgan et al., 2019). Michael Mazarr similarly insists that ambiguity itself is the primary strategic effect in grey-zone operations, because it disorganises lawful response pathways and disperses responsibility across institutions (Mazarr, 2015).

Information operations scholarship advances a closely related claim. W. Lance Bennett and Steven Livingston describe a "disinformation order" whose salient feature is the erosion of shared standards of truth and trust in institutional authority (Bennett & Livingston, 2018). Thomas Rid situates this within the longer history of active measures, emphasising that strategic deception often aims to degrade governance capacity rather than to win arguments in the public sphere (Rid, 2020). Peter Pomerantsev's work has revealed Russia's weaponization of unreality to disorient, demoralise, and ultimately disarm its own population, lessons that were subsequently applied by Russia against Americans, Europeans, and others (Pomerantsev, 2019). This is in part accomplished with a so-called "firehose of falsehood" (Paul & Matthews, 2016). The so-called political technologists' goal is to overload comprehension to foster cynicism, conspiracism, or complacency. Kathleen Hall Jamieson and Joseph Cappella show empirically that certain forms of political media and partisan opinion ecosystems can activate cynicism, reinforce mistrust of mainstream information sources, and reduce civic participation; by extension, such effects may be strategically valuable for an enemy. In a crisis when public trust and cooperation are essential, targeted countries may be paralyzed by spiralling societal cynicism (Cappella & Jamieson, 1997; Jamieson & Cappella, 2008). Yochai Benkler, Robert Faris, and Hal Roberts describe an asymmetric media ecosystem in which dense partisan networks amplify identity-confirming narratives and weaken corrective mechanisms; read alongside information-overload models, their findings suggest that networked propaganda often works less by direct persuasion than by saturating the information environment and insulating audiences from authoritative correction (Benkler, Faris, and Roberts, 2018). Peer-reviewed crisis and platform research further indicates that participatory and distributed dynamics make information operations resilient, because they function as collaborative ecosystems rather than centrally broadcast campaigns (Starbird et al., 2019).

Legal scholarship has developed in parallel, often without being integrated into hybrid warfare frameworks. Orde Kittrie defines lawfare as the use of law as a weapon of war and argues that legal processes can impose asymmetric costs through delay, reputational pressure, and procedural burden even when they do not produce courtroom victories (Kittrie, 2016). Karen Alter's work on the political consequences of international adjudication shows how litigation can reshape state behaviour by creating risk and compliance burdens before final judgments are rendered (Alter, 2014). Related scholarship on international courts further demonstrates that legal proceedings can change institutional incentives by altering expectations of legitimacy, compliance, and future legal exposure (Helfer and Alter, 2013).

Critical infrastructure scholarship has shifted from general vulnerability arguments to system effects and governance chokepoints. James Andrew Lewis argues that critical infrastructure risk is magnified by institutional dependencies and regulatory chokepoints, which adversaries can exploit to generate cascading costs (Lewis, 2020). Work on critical undersea infrastructure similarly highlights how cable incidents and suspicious vessel activity can activate private-sector coordination, redundancy planning, insurance review, and political concern even when damage or attribution remains uncertain (Monaghan et al., 2023; Hoorman and Vincent, 2024). Energy-security scholarship likewise shows that perceived reliability risks can produce political and economic consequences beyond direct physical damage (Goldthau and Sitter, 2015).

Maritime and seabed governance literature adds the intermediary layer that is essential to the present research question. Christian Bueger and Timothy Edmunds argue that maritime security governance increasingly depends on diffuse public-private coordination among state agencies, international organizations, shipping interests, private security companies, and other non-state actors; this supports the broader point that non-state and commercial actors can shape how maritime risks are identified, prioritized, and acted upon (Bueger and Edmunds, 2017). Recent policy analysis on undersea infrastructure similarly emphasises fragmented ownership, commercial operation, civil-military coordination challenges, and the difficulty of converting suspicious activity into timely response thresholds (Monaghan et al., 2023; Hoorman and Vincent, 2024).

The integrative gap in the literature is increasingly acknowledged even by analysts sympathetic to the hybrid framework. John Wither observes that hybrid warfare discussions often list multiple domains but rarely model deliberate temporal coordination across them as an operational pattern (Wither, 2016). This literature supports the claim that synchronisation, not novelty of individual tools, is the distinctive mechanism that needs systematic explanation.

Georgia-focused scholarship provides the empirical anchor for the Georgia-as-early-warning argument. Edward Boyle characterizes borderization as the materialization of a previously theoretical or administrative boundary through fences, markers, barbed wire, and patrols, a process that can move the Georgian–South Ossetian boundary deeper into previously Georgian-controlled territory and normalize incremental changes on the ground (Boyle, 2017). Related analyses describe this practice as a form of creeping annexation or the creation of new “facts” on the ground, suggesting how repeated administrative and material acts can consolidate territorial change without triggering a conventional escalation response. De Waal likewise treats the Georgian theatre as a setting in which unresolved status, constrained deterrence, and cyclical international attention make coercive routines unusually visible (de Waal, 2018).

Finally, European governance and regulatory literature clarifies why legal and institutional friction is not incidental but structurally predictable. EU cybersecurity rules such as the NIS2 Directive create reporting, coordination, and supervisory obligations that are essential for resilience but can also impose time-sensitive classification and compliance burdens during complex incidents (European Union, 2022). Policy analysis on foreign information manipulation and interference likewise emphasises that modern influence operations exploit institutional seams, especially during crises that require rapid, trusted communication (European External Action Service, 2023).

Taken together, these sources establish a sophisticated but fragmented understanding of hybrid coercion. What remains missing is an integrated account of how infrastructure interference, lawfare, and information operations are deliberately synchronised to generate compound economic, legal, and societal effects. Addressing this gap is the central contribution of the present study.

3. Materials and Methods

This article advances a theory of synchronised hybrid coercion in which physical disruption, legal pressure, and information manipulation operate as a coupled system rather than as parallel or additive

instruments. The theoretical claim is not that these tools are novel, but that their strategic effect emerges from deliberate temporal coordination that exploits institutional fragmentation, legal precaution, and crisis-driven dependence on trust. This approach builds on existing hybrid warfare and gray-zone theories while addressing their limitations in explaining compound effects across governance systems.

The starting point is Frank G. Hoffman's conceptualisation of hybrid warfare. The present theory extends this foundation by treating time as a strategic variable. Rather than asking whether an action is military or non-military, the theory asks how actions across domains are synchronised to amplify uncertainty and otherwise weaken the target.

This temporal focus draws on gray-zone scholarship that emphasises ambiguity as an operational effect. The present theory builds on this insight by specifying how ambiguity is produced through coordination rather than through any single ambiguous act.

Institutional theory provides the second pillar. James March and Johan Olsen's work on institutional behaviour demonstrates that organisations respond most slowly under conditions of rule conflict and procedural uncertainty (March and Olsen, 1989). In hybrid campaigns, legal venues, regulatory frameworks, and crisis-response protocols are deliberately activated simultaneously, forcing institutions to resolve competing obligations under pressure. This produces what the theory conceptualises as administrative saturation, a condition in which compliance requirements and verification standards exceed decision-making capacity.

Lawfare functions within this framework as a timing instrument rather than merely a legal tactic. Orde Kittrie notes that its power lies in process rather than outcome (Kittrie, 2016). The present theory conceptualises litigation bursts as temporal anchors that lock institutions into procedural timelines precisely when rapid response is required. Karen Alter's analysis of international adjudication supports this view by showing how legal proceedings reshape behaviour long before judgments are rendered (Alter, 2014).

Information operations supply the third coordinating mechanism. W. Lance Bennett and Steven Livingston describe a "disinformation order" in which institutional authority erodes as verification demands outpace communication capacity (Bennett and Livingston, 2018). Thomas Rid's historical analysis of active measures reinforces this interpretation by framing influence operations as efforts to degrade governance rather than persuade populations (Rid, 2020). Within the proposed theory, information operations function as accelerants that intensify uncertainty generated by physical disruption and legal contention, particularly during crises that require trusted guidance.

Critical infrastructure disruption provides the triggering mechanism. James Andrew Lewis argues that modern infrastructure vulnerability lies less in physical fragility than in institutional dependencies and regulatory chokepoints (Lewis, 2020). This insight aligns with the article's focus on downstream effects: insurance review, regulatory reporting, crisis communication, and political risk often determine the practical consequences of ambiguous incidents. The theory therefore treats infrastructure interference as a means of activating legal and informational stress rather than as an end in itself.

These elements combine into a model of synchronised hybrid coercion with three core propositions. First, strategic effect arises from timing rather than scale. Second, ambiguity is produced through cross-domain interaction rather than through isolated deniable acts. Third, deterrence fails when legal and regulatory systems are not designed for coordinated activation under time pressure. Georgia functions within this theoretical model as an early-warning environment where these dynamics are observable in compressed form due to limited deterrence and high institutional exposure.

The theoretical contribution of this article lies in reframing hybrid coercion as a governance stress test rather than a threshold problem. By integrating insights from hybrid warfare theory, institutional analysis, lawfare scholarship, and information studies, the theory explains why synchronised campaigns generate disproportionate economic, legal, and societal effects without triggering conventional escalation. This framework provides the analytical basis for the operational legal playbook developed in the subsequent sections.

This article adopts a theoretical and documentary research design intended to operationalise the conceptual framework of synchronised hybrid coercion developed in the Theory section. The methodological objective is to translate abstract propositions about timing, ambiguity, and institutional stress into a structured analytical approach capable of practical application and further scholarly extension. The methods therefore focus on conceptual integration, procedural analysis, and pattern reconstruction rather than on hypothesis testing through quantitative measurement.

The first methodological component consists of structured theoretical synthesis across disciplines. Scholarship on hybrid warfare, lawfare, information operations, critical infrastructure security, and institutional governance is systematically compared to identify how different fields conceptualise sequencing, uncertainty, and response delay. This synthesis follows the logic of structured and focused comparison developed by Alexander George and Andrew Bennett, which allows theoretical refinement while preserving contextual specificity (George and Bennett, 2005).

The second component involves documentary analysis of legal and regulatory systems as operational environments. International legal instruments, European regulatory frameworks, court procedures, sanctions regimes, and cybersecurity reporting obligations are examined to identify procedural thresholds, verification requirements, and timelines that shape institutional behaviour during crises. Karen Alter's analysis of international adjudication informs this approach by demonstrating that legal and regulatory effects emerge at the moment of process initiation rather than only at final adjudication (Alter, 2014). More recent legal scholarship reinforces that procedural density and jurisdictional overlap amplify uncertainty and administrative burden under stress conditions (Helfer and Alter, 2013).

Within this documentary framework, legal activity is treated as an operational variable rather than as an exogenous constraint. Investment arbitration, maritime claims, human rights litigation, and sanctions challenges are analysed for their capacity to impose delay, increase compliance costs, and condition institutional risk perception. This approach builds on Orde Kittrie's conception of lawfare as process-based coercion and is extended through recent peer-reviewed work showing how clustered litigation

produces cumulative regulatory effects across jurisdictions (Kittrie, 2016). Legal events are therefore analysed for timing and interaction rather than for legal outcome.

The third component incorporates process-oriented reconstruction of physical disruption. Rather than compiling an exhaustive incident dataset, the study reconstructs recurring sequences involving seabed cable interference, rail and electricity grid disruption, GPS spoofing, and borderisation practices. These phenomena are analysed for their downstream institutional and regulatory effects rather than for their technical characteristics. James Andrew Lewis's work on infrastructure vulnerability informs this approach by emphasising that strategic disruption exploits institutional dependencies rather than physical fragility alone (Lewis, 2020). Recent infrastructure governance research further supports treating uncertainty and attribution ambiguity as central analytical variables (Lewis, 2020).

A fourth component examines information operations and crisis communication as coordinating mechanisms. Documentary analysis of public advisories, platform messaging, and broadcast communications is used to assess narrative convergence, provenance ambiguity, and timing relative to physical and legal stressors. This approach follows W. Lance Bennett and Steven Livingston's framework that conceptualises disinformation as a systemic condition eroding institutional authority and verification capacity (Bennett and Livingston, 2018). Recent peer-reviewed communication research further demonstrates that crisis contexts magnify the governance impact of conflicting or deceptive messaging by increasing dependence on authoritative guidance (Freelon and Wells, 2020).

This information-focused stage also provides the methodological entry point for incorporating China into the study. Chinese state media output, diplomatic statements, open-source studies of Sino-Russian narrative convergence, sanctions-related economic research, dual-use trade analysis, and scholarship on digital dependence must be examined to determine how Chinese narratives, trade relationships, financial adaptation, and technology ecosystems interact with Russian coercive activity at the level of institutional effect. China is not treated as interchangeable with Russia or as a direct participant in every Russian-origin action. Rather, its relevance is assessed through the extent to which Chinese-linked narratives, commercial channels, technological dependencies, and diplomatic framing sustain, legitimise, cushion, or complicate European responses to Russian pressure.

The methodological value of this addition lies in distinguishing operational authorship from strategic enablement. The study therefore evaluates China-linked material through three related indicators: 1.) convergence with Russian claims concerning NATO, sanctions, Western responsibility, and the war in Ukraine, 2.) economic and technological support that reduces Russia's exposure to sanctions or export controls, and 3.) European dependency on Chinese-linked technology, infrastructure, or supply chains that introduces caution into crisis decision-making.

Cross-domain interaction is assessed through temporal sequencing analysis. Events and procedural processes across physical, legal, and informational domains are analytically ordered to identify clustering, lag effects, and reinforcement dynamics. This sequencing logic reflects Michael Mazarr's argument that ambiguity and delay function as strategic effects in gray-zone competition rather than as incidental by-products (Mazarr, 2015).

Georgia is incorporated as a theoretical probe rather than a representative case study. Edward Boyle's analysis of borderisation provides the basis for treating Georgia as an environment where incremental coercion, legal ambiguity, and administrative normalisation are repeatedly observable (Boyle, 2017). De Waal similarly supports treating Georgia as an early-warning context in which unresolved status, administrative friction, and limited enforcement make coercive practices unusually visible (de Waal, 2018). The case is used to test internal coherence of the synchronisation framework and to generate hypotheses about diffusion and institutional adaptation.

Finally, the study incorporates documentary analysis of cybersecurity incident reporting and regulatory escalation, including post-NIS2 governance. Regulatory texts and interpretive guidance are examined to identify how reporting thresholds, compliance obligations, and data-sharing constraints affect response timing. NIS2 is treated as an example of a resilience framework whose mandatory reporting and coordination requirements may also create administrative load during complex incidents (European Union, 2022).

The methodological outcome of this approach is an operational analytical framework rather than a dataset. The study develops criteria for identifying synchronisation, indicators of legal and regulatory overload, and conditions under which ambiguity shifts from deterrent to destabilising. These outputs are designed to be replicable and adaptable, providing a foundation for future comparative research and applied policy analysis on hybrid coercion and institutional resilience.

4. Discussion of Findings

The analysis identifies a recurring pattern in which physical disruption, legal and regulatory processes, and information operations cluster within compressed timeframes. The pattern is the strongest where infrastructure anomalies, attribution uncertainty, and crisis communication demands arise together. The significance is not the scale of any single incident, but the way limited actions activate several institutional systems at once.

Across the examined domains, legal and regulatory procedures amplify pressure by imposing verification, reporting, consultation, and compliance obligations before final attribution or adjudication. Information operations then intensify the burden by contesting authoritative guidance and increasing the cost of public communication. Together, these effects produce administrative saturation: delayed decisions, fragmented authority, precautionary behaviour, and rising economic costs.

Infrastructure interference functions as a trigger rather than an end in itself, because even ambiguous disruption can activate insurance review, safety protocols, procurement delay, and public messaging requirements. Georgia illustrates this logic in long-duration form. Borderisation, legal ambiguity, cyber activity, electromagnetic interference, and narrative pressure interact over time, showing how coercion can become routinised without decisive escalation.

The findings support a model of hybrid coercion as governance stress rather than a threshold problem. Deterrence therefore depends on procedural coordination, faster attribution pathways, and pre-agreed response thresholds, not only on declaratory policy.

Russia's hybrid coercion provides the strategic context for the domain-specific analysis that follows. Its effectiveness lies in exploiting procedural dependence: evidentiary standards, legal review, safety obligations, inter-agency coordination, and public accountability slow response under ambiguity, even when responsibility is politically understood. The sections below therefore focus less on whether individual tactics are novel than on how infrastructure, legal, informational, cyber, and electromagnetic pressures interact to make European action slower, costlier, and more politically fraught (Giles, 2016; Monaghan, 2019; Galeotti, 2016).

4.1. Physical Infrastructure Interference as a Governance Stress Mechanism

Physical interference with critical infrastructure occupies a central position in Russia's hybrid coercion model because it activates regulatory, legal, and economic systems that are inherently slow, fragmented, and risk-averse. Russia systematically targets infrastructure that is civilian or dual-use, privately operated, and governed by overlapping national and international regimes. These characteristics ensure that response responsibility is dispersed across multiple actors, complicating coordination and delaying decisive action.

Undersea telecommunications cables provide a paradigmatic example of this operational logic. These cables carry the vast majority of European digital traffic and underpin financial markets, government communications, emergency services, and military command systems. Despite their criticality, responsibility for their protection is fragmented among coastal states, private consortia, insurers, and international legal frameworks. European officials and media investigations have reported repeated activity by Russian intelligence-linked vessels near European cable routes and other critical undersea infrastructure, creating situations in which suspicious activity is visible but not easily classifiable as hostile (Hoorman and Vincent, 2024; Monaghan et al., 2023; Bueger and Edmunds, 2017). Even without confirmed sabotage, such activity compels inspections, traffic rerouting, insurance notifications, and regulatory review. These processes generate delay and cost across dependent systems, regardless of whether physical damage is ultimately found.

From a coercive perspective, the value of this activity lies not in denying connectivity, but in forcing precautionary governance. Authorities must act conservatively in the face of uncertainty, prioritising safety and compliance over speed. Policy analysis on undersea infrastructure security emphasises that ownership, repair responsibility, evidence collection, and civil-military coordination are fragmented, making rapid response difficult under conditions of ambiguity (Monaghan et al., 2023; Hoorman and Vincent, 2024). Russia exploits this mismatch between risk sensitivity and response capability to impose persistent institutional strain.

Energy infrastructure exhibits similar vulnerabilities. Europe's electricity grids and gas networks are highly interconnected across borders and governed by dense regulatory regimes designed to prevent

cascading failures. Minor anomalies, unexplained outages, or suspicious disruptions activate mandatory reporting, inspection, and coordination procedures that slow response and heighten political sensitivity. Even when technical resilience prevents prolonged outages, the political and economic consequences of perceived energy insecurity can be significant (Goldthau and Sitter, 2015). Russia benefits from this sensitivity, particularly during periods of high demand or geopolitical tension, because it amplifies the impact of limited interference.

Rail networks and logistics systems are likewise susceptible to interference that manifests as technical malfunction rather than overt attack. Signal failures, control system anomalies, or unexplained disruptions can halt freight and passenger movement without clearly qualifying as sabotage. These incidents trigger safety reviews and inspections that delay recovery and impose economic cost. Because responsibility is shared among operators, regulators, and safety authorities, decision-making becomes sequential rather than parallel, further slowing response (Lewis, 2020).

Navigation interference, particularly GPS spoofing and jamming, extends this logic into the electromagnetic domain. Temporary manipulation of navigation signals affects civilian aviation and maritime traffic, forcing rerouting, grounding, and heightened verification. Reporting on Russian-linked GPS spoofing and technical interference shows how such activity can affect commercial shipping and civilian navigation while remaining difficult to attribute in real time (Burgess, 2019). Even when interference is transient, safety obligations compel conservative response, ensuring that the burden falls on governance systems and commercial operators rather than on security forces.

Across these sectors, Russia's method is consistent. Physical actions are ambiguous, reversible, and calibrated to remain below military thresholds. The downstream institutional consequences are predictable, costly, and cumulative. Infrastructure is not targeted for destruction, but for its capacity to trigger regulatory, legal, and economic processes that impose delay, inflate risk, and erode confidence. In this sense, physical interference functions as a governance stress mechanism, initiating cascades that extend far beyond the point of initial disruption.

4.2. Legal and Regulatory Systems as Instruments of Time-Based Coercion

Legal and regulatory systems form a central operational domain in Russia's hybrid coercion model because they impose mandatory procedures that cannot be bypassed without undermining democratic legitimacy. Unlike physical disruption, which creates immediate operational consequences, legal pressure operates through delay, risk aversion, and procedural saturation. Russia exploits the fact that European governance systems are designed to privilege lawful process over speed, particularly in areas involving infrastructure safety, human rights, commercial liability, and sanctions enforcement.

A recurring feature of Russian hybrid activity is the clustering of legal actions around periods of physical disruption or political stress. These actions include investment arbitration claims challenging emergency regulatory measures, maritime litigation contesting jurisdiction following ambiguous incidents at sea, human rights petitions alleging violations arising from security measures, and sanctions challenges seeking exemptions, delisting, or compensation (Kittrie, 2016). The significance of these legal actions

does not lie primarily in their likelihood of success. Instead, it lies in the procedural obligations they trigger from the moment they are initiated.

Once legal proceedings begin, institutions are required to preserve documents, consult legal counsel, notify insurers and regulators, and often suspend or review contested actions. Procurement decisions for infrastructure repair may be delayed pending liability clarification. Emergency measures may be softened to reduce litigation risk. Regulatory authorities may hesitate to act decisively in the absence of clear legal cover. As Alter has demonstrated, the political and behavioural effects of legal proceedings begin well before adjudication, shaping institutional behaviour through anticipation and precaution (Alter, 2014).

This procedural burden is amplified when legal pressure is applied across multiple forums simultaneously. European governance is characterised by overlapping jurisdictions and regulatory mandates. A single incident can therefore trigger parallel proceedings in national courts, international arbitration panels, and human rights bodies. Each forum operates according to distinct rules and timelines, fragmenting institutional attention and complicating coordination. The result is administrative congestion rather than legal resolution (Helfer and Alter, 2013).

From a coercive standpoint, this dynamic is advantageous because it externalises cost. The responding state bears the administrative, financial, and political burden of compliance, while Russia retains deniability and strategic flexibility. Legal and regulatory systems become mechanisms through which pressure is institutionalised rather than resisted. Time itself becomes the weapon. Delay accumulates, costs rise, and the window for decisive response narrows without any single action crossing a clear escalation threshold.

4.3. Information Operations as Institutional Disruption

Information operations constitute the third pillar of Russia's hybrid coercion model, but their function is frequently misunderstood. Rather than aiming primarily to persuade populations of specific falsehoods, Russian information operations are designed to disrupt institutional authority, particularly during moments when public compliance and trust are most critical. The objective is not belief, but hesitation.

Russia's information activity is structured to exploit crisis conditions. During infrastructure disruptions, energy shortages, extreme weather events, or periods of heightened legal uncertainty, public authorities must issue guidance rapidly and credibly. Russian information operations intervene at precisely these moments by injecting contradictory messages, forged advisories, manipulated translations, and selectively edited official statements into the information environment (Rid, 2020). These messages circulate through a mix of state-aligned outlets, fringe media, and encrypted platforms, complicating attribution and response.

A key methodological feature of this approach is targeting institutional dependency on trust. Democratic governance relies on voluntary compliance with official guidance. When citizens are unsure which messages are authentic, compliance drops even in the absence of widespread belief in false narratives. Officials, in turn, slow communication to verify accuracy and consult legal advisors, reinforcing delay.

This interaction between information ambiguity and procedural caution produces systemic disruption that exceeds the impact of any single false claim (Pomerantsev, 2019).

Minority-language communities are frequently targeted because official communication capacity is the weakest there. Translations lag, trusted intermediaries are fewer, and verification is more difficult. Russian messaging exploits these gaps by circulating forged or misleading advisories that mimic official formats. The result is not mass persuasion, but fragmentation of response across linguistic and social groups.

Information operations are the most effective when synchronised with physical disruption and legal uncertainty. Physical incidents create urgency. Legal proceedings constrain institutional speech. Information manipulation exploits both by eroding confidence at the moment of peak dependence on authority. Bennett and Livingston describe this dynamic as a systemic condition rather than a collection of falsehoods, where the cumulative effect is declining institutional legitimacy rather than ideological conversion (Bennett and Livingston, 2018).

From Russia's perspective, information operations serve as an accelerant. They magnify uncertainty generated by other domains and ensure that institutional response remains slow, cautious, and contested. The burden of verification and correction falls on public authorities, while the cost of producing ambiguity remains low. Over time, this erodes confidence in crisis governance and normalises confusion as an expected feature of public life.

4.4. China as a Strategic Enabler and Parallel Actor in Europe's Hybrid Environment

China's role in Europe's hybrid environment is structurally different from Russia's but strategically consequential. Whereas Russia applies direct coercive pressure through ambiguity, disruption, and deniable action, China functions primarily as a strategic enabler and parallel actor whose activities shape the conditions under which coercion can be sustained over time. China's approach emphasises persistence, institutional embedding, and leverage derived from economic and technological interdependence rather than episodic shock. This distinction is central to understanding why Chinese activity often appears non-coercive in isolation while still contributing to cumulative governance stress (Rolland, 2020).

Chinese state strategy prioritises long-term positioning within systems that European governance depends upon, including telecommunications infrastructure, digital platforms, research and academic networks, supply chains, and media distribution ecosystems. These engagements are typically framed as commercial, cultural, or diplomatic, and they frequently comply with existing legal and regulatory frameworks. However, their strategic value lies in the dependencies they create. During periods of crisis or heightened geopolitical tension, these dependencies constrain European policy choices by increasing the perceived cost of confrontation or disengagement (Seaman et al., 2021).

From a hybrid coercion perspective, China's contribution lies in broadening the battlespace rather than initiating disruption. When European institutions must simultaneously manage Russian-origin physical

or legal pressure and Chinese-linked economic or informational considerations, institutional attention is fragmented. Different parts of the state operate under different legal mandates, timelines, and risk thresholds. This fragmentation aligns with the core mechanics of hybrid coercion by slowing coordinated response and complicating prioritization (Farrell and Newman, 2019; Seaman et al., 2021).

China's role does not require formal coordination with Russia to be strategically meaningful. Parallel state practices that converge in effect can generate pressure comparable to coordinated action. The absence of explicit coordination further complicates attribution and response, reinforcing uncertainty within European governance systems.

4.5. Information Operations and Sino-Russian Narrative Convergence

The most visible and analytically tractable area of Sino-Russian interaction in Europe lies in the information domain. Chinese state media, diplomatic messaging, and affiliated outlets frequently promote narratives that align with or reinforce Russian framing during periods of geopolitical tension involving Europe, NATO, sanctions, or the war in Ukraine. This convergence does not take the form of identical messaging but rather of discursive alignment, in which similar causal stories, blame attribution, and normative claims are advanced through distinct channels (Bahenský et al., 2023).

Empirical analysis of media output demonstrates that Chinese state-controlled outlets often echo Russian narratives portraying NATO expansion as destabilising, sanctions as illegitimate, and Western policy as hypocritical or reckless. These narratives are typically embedded within broader Chinese discourses emphasising sovereignty, non-interference, and multipolarity. By reframing Russian claims within a Chinese rhetorical structure, these outlets allow Russian narratives to circulate through channels that appear less directly associated with Moscow, increasing reach and plausibility (Hellström et al., 2024).

This convergence has methodological significance for European information governance. Democratic institutions rely heavily on source identification and intent assessment when responding to disinformation. When similar narratives emerge from two distinct state media ecosystems, institutions must determine whether alignment reflects coincidence, shared worldview, or deliberate coordination. This uncertainty raises the evidentiary threshold for response and delays countermeasures, particularly during crises when rapid communication is essential (European External Action Service, 2023).

Chinese diplomatic messaging reinforces this effect. Official statements and social media communications frequently adopt rhetorical frames that parallel Russian claims regarding Western responsibility for instability and the illegitimacy of sanctions or security assistance. While China does not endorse all Russian actions, this rhetorical alignment contributes to a permissive discursive environment in which Russian coercion is contextualised as understandable or defensive rather than aggressive. The cumulative effect is erosion of narrative clarity and increased institutional hesitation (Hellström et al., 2024; European External Action Service, 2023).

4.6. Economic and Technological Enablement as Structural Support for Coercion

China's most consequential contribution to the European hybrid environment lies in the domain of economic and technological enablement. European sanctions, export controls, and regulatory restrictions are designed to impose economic cost and constrain hostile behaviour. China's willingness to maintain trade, provide alternative markets, and supply technological substitutes reduces the effectiveness of these measures, particularly with respect to Russia.

Analyses of interdependence and Chinese economic statecraft demonstrate how alternative markets, financial channels, and technological supply chains can reduce the coercive effect of Western restrictions and complicate European attempts to isolate hostile actors (Farrell and Newman, 2019; Seaman et al., 2021). From a hybrid perspective, this matters because coercion is effective only if it can be sustained over time. Economic resilience underwrites strategic persistence.

In the technological domain, European security assessments have raised concerns regarding Chinese dual-use technologies, including telecommunications infrastructure, surveillance systems, and data-processing platforms. The presence of such technologies within European systems creates dependencies that complicate governance and incident response. Regulatory authorities must balance security concerns against legal obligations, economic interests, and contractual commitments. This tension introduces delay and caution into decision-making processes, particularly during crises (Polyakova & Meserole, 2019).

Even when Chinese technologies are not transferred directly to Russia, their existence as alternative supply chains weakens the leverage of European export controls and sanctions regimes. The availability of substitutes reduces the deterrent effect of restrictions and increases the difficulty of economically isolating hostile actors. In this way, China indirectly contributes to the sustainability of Russia's hybrid coercion by lowering its long-term costs (Farrell & Newman, 2019).

5. Strategic Implications of Sino-Russian Parallelism

The interaction between Russian coercive activity and Chinese state practice produces a strategic environment in which European institutions face persistent, multidirectional pressure. Russia generates acute disruption through physical interference, legal contestation, and information manipulation. China expands the informational, economic, and technological space in which that disruption can persist with fewer constraints. The two approaches are complementary rather than identical.

This parallelism has significant implications for governance resilience. European institutions are organised around sector-specific mandates, legal regimes, and regulatory timelines. Hybrid coercion exploits this fragmentation by ensuring that pressure arrives simultaneously across domains governed by different rules. Russian and Chinese activities do not need to be synchronised tactically to be synchronised in effect. Their interaction stretches institutional capacity, complicates attribution, and normalises contestation across domains (Mazarr, 2015).

Understanding China's role as a secondary but structurally significant actor is therefore essential for interpreting the broader hybrid environment. It clarifies why countering coercion cannot be reduced to deterring a single actor or responding to isolated incidents. Instead, it requires addressing the conditions under which parallel state practices interact to impose cumulative governance stress.

5.1. Georgia as a Long-Duration Laboratory of Russian Hybrid Coercion

Georgia constitutes a paradigmatic case of long-duration hybrid coercion in which the Russian Federation has applied coordinated pressure across territorial, legal, cyber, electromagnetic, informational, and administrative domains over an extended period of time. Unlike episodic hybrid campaigns observed in larger European states, the Georgian case is characterised by continuity, repetition, and institutional exposure. This continuity allows the internal mechanics of hybrid coercion to be observed with unusual clarity, particularly under conditions where deterrence is weak, enforcement mechanisms are limited, and ambiguity can be sustained indefinitely.

Following the August 2008 war, Russia deliberately refrained from pursuing either full territorial annexation or a comprehensive political settlement. Instead, it adopted a strategy that multiple scholars describe as a frozen conflict or a managed non-resolution (Bescotti, 2019; Kelmendi and Kapanadze, 2025). The unresolved status in the post-Soviet space functions as a mechanism of control rather than a failure of diplomacy, enabling the dominant power to modulate pressure without triggering decisive counteraction (Bescotti, 2019; de Waal, 2018; Kelmendi and Kapanadze, 2025). In Georgia, this strategy transformed the ceasefire framework into an operational platform for continuous coercion.

This approach reflects a broader Russian preference for controlling escalation by fragmenting it across domains and time. Rather than concentrating force, Russia distributes pressure in ways that compel Georgian institutions to respond repeatedly through legal, administrative, and diplomatic channels. The cumulative effect is governance exhaustion rather than crisis escalation.

5.2. Borderisation as Incremental Territorial and Administrative Coercion

Borderisation constitutes the most durable and structurally revealing mechanism of Russian hybrid coercion in Georgia. It is not merely a territorial practice, but a method of administrative governance through incremental physical control, designed to impose cumulative political, legal, and humanitarian costs while remaining below thresholds that would provoke decisive international intervention. As such, borderisation exemplifies how hybrid coercion functions over time when ambiguity is preserved and escalation is deliberately avoided.

The practice emerged gradually in the years following the 2008 war, becoming particularly systematic from around 2011 onward. Rather than attempting formal annexation or negotiated boundary settlement, Russian forces and proxy security actors began installing fences, barbed wire, surveillance equipment, signage, and patrol infrastructure along the administrative boundary lines separating Georgian-controlled territory from Abkhazia and South Ossetia. These actions were framed as technical or security-related adjustments, often justified through claims of crime prevention or stabilisation. Each individual

installation appeared minor and reversible, yet their cumulative effect was spatially transformative (de Waal, 2018).

Scholars emphasise that borderisation operates through temporal fragmentation. Boyle characterizes it as the materialisation of a contested administrative boundary, while its effectiveness lies in the slow production of facts on the ground that cannot easily be contested in real time through diplomatic or legal means (Boyle, 2017). Because each adjustment is small, responses are typically delayed, procedural, or symbolic. Over time, this allows physical control to advance without triggering crisis framing or sustained external pressure.

The material consequences of borderisation are extensive and measurable. Agricultural land that had been farmed for generations becomes inaccessible overnight. Irrigation channels and drainage systems are severed, rendering remaining land less productive. De Waal describes how boundary enforcement and restricted movement create humanitarian, administrative, and infrastructure dilemmas for Georgian authorities and local communities (de Waal, 2018). Roads connecting villages to markets, schools, and medical services are cut, forcing residents to undertake long detours or abandon livelihoods altogether.

Detention practices are integral to this system. Civilians are routinely detained for illegal border crossing despite the absence of a legally defined international border. These detentions are processed administratively rather than militarily, reinforcing their normalisation. Detainees are typically released after fines or short-term confinement, but the practice generates persistent fear and uncertainty among border communities. In this sense, such detentions operate as coercive signalling, teaching populations where movement is permissible through punishment rather than enforceable legal clarity.

From a legal perspective, borderisation exploits a jurisdictional void. The administrative boundary lines are not recognised as international borders under international law, yet they are enforced as such by Russian and proxy forces. This creates a situation in which Georgian legal remedies are limited and international judicial mechanisms lack enforcement capacity. Appeals to international organisations produce monitoring reports and diplomatic statements, but no material reversal. The absence of an enforcement mechanism allows incremental change to solidify into de facto reality.

Institutionally, this produces what multiple analysts describe as governance fatigue. Georgian state agencies devote disproportionate resources to managing micro-incidents, including detentions, access disputes, and humanitarian complaints. Each incident requires documentation, diplomatic communication, and administrative processing, yet none leads to resolution. Over time, this shifts institutional behaviour from contestation to management. What was initially treated as an exceptional violation becomes routinised administrative work.

Borderisation also has important symbolic and psychological effects. The physical presence of fences, cameras, and armed patrols communicates permanence and inevitability. For local populations, this undermines confidence in the state’s ability to protect territory and citizens. For Georgian institutions, it reinforces a perception that escalation will not produce reversal, encouraging restraint even when

incremental loss continues. In this dynamic, time works in favour of the stronger actor by allowing control to expand without direct confrontation (de Waal, 2018).

Crucially, borderisation is not isolated from other coercive domains. It interacts with legal ambiguity, information pressure, cyber activity, and electromagnetic interference to form a coherent system. Physical markers define space. Legal indeterminacy prevents redress. Detentions enforce compliance. Narrative framing minimises responsibility. Together, these elements demonstrate how Russia uses administrative practices rather than overt force to reshape territorial reality while maintaining plausible deniability.

From an analytical standpoint, borderisation illustrates the core logic of hybrid coercion. It shows how incrementalism substitutes for escalation, how administrative routines substitute for military occupation, and how ambiguity substitutes for legitimacy. The Georgian case demonstrates that when such practices are sustained over time, they can produce durable territorial and governance outcomes without triggering decisive external response. This is why borderisation is not merely a regional phenomenon, but a foundational example of how hybrid coercion operates in practice.

5.3. Legal Indeterminacy and the Weaponisation of Non-Resolution

Legal indeterminacy is not a by-product of Russia's approach to Georgia. It is a deliberately sustained instrument of coercion that transforms unresolved conflict into a permanent governance burden. Rather than seeking juridical clarity, negotiated settlement, or formal annexation, Russia has consistently acted to preserve an intermediate legal condition in which authority, jurisdiction, and responsibility remain contested. This condition enables continuous pressure without triggering escalation thresholds that would follow either recognised annexation or open warfare.

Following the 2008 ceasefire, the legal framework governing Georgia's occupied territories was left intentionally incomplete. The ceasefire arrangements halted large-scale hostilities but did not establish a binding political settlement, internationally recognised borders, or enforcement mechanisms capable of compelling compliance. Russia has since treated this absence of final status not as a temporary gap but as an operational opportunity. As several legal scholars note, unresolved status allows the dominant power to exercise control while deflecting responsibility, since obligations remain ambiguous and enforcement diffuse (Helfer & Alter, 2013).

At the core of this strategy is the conversion of non-resolution into routine administration. Russian and proxy authorities enforce de facto jurisdiction through administrative practices rather than formal legal acts. Detentions, access restrictions, and boundary enforcement are framed as law-enforcement measures, even though the underlying legal basis is undefined. This framing forces Georgian authorities and international observers to respond within legal vocabularies that are poorly suited to contesting incremental coercion. Each incident becomes a technical dispute rather than a political violation (de Waal, 2018).

International law provides limited leverage in this environment. While Georgia consistently asserts sovereignty over Abkhazia and South Ossetia, international courts and monitoring mechanisms lack enforcement capacity. Cases brought before international bodies generate findings, reports, and condemnations, but they do not compel reversal on the ground. Russia, by maintaining ambiguity over jurisdiction and status, avoids clear violations that would trigger enforceable remedies. As Alter observes more generally, international adjudication often shapes discourse without altering power relations when enforcement is absent (Alter, 2014).

This legal vacuum produces asymmetric effects. Russia benefits from ambiguity because it can act administratively while denying sovereign responsibility. Georgia, by contrast, is constrained by its commitment to international law and its reliance on legal forums for redress. Every response must be framed in terms of legality, proportionality, and diplomatic restraint. This asymmetry transforms law from a shield into a source of vulnerability. Legal process becomes a channel through which delay and caution are imposed rather than a means of protection (Kittrie, 2016).

Over time, this dynamic generates institutional fatigue. Georgian ministries, courts, and diplomatic services devote significant resources to documenting incidents, filing protests, responding to monitoring missions, and supporting affected civilians. Yet these efforts rarely produce tangible change. The repetition of unresolved cases erodes confidence in legal remedies and shifts institutional priorities from political contestation toward bureaucratic management (de Waal, 2018).

Russia reinforces this fatigue by maintaining the appearance of legal normalcy. Administrative procedures are followed. Detentions are processed. Fines are issued. Boundaries are marked. This creates a simulacrum of legality that is difficult to challenge without rejecting the entire framework of legal order. Over time, coercion becomes absorbed into ordinary governance routines, making resistance appear disruptive rather than defensive (de Waal, 2018).

Legal indeterminacy also interacts with other coercive domains. Borderisation relies on the absence of a legally enforceable boundary. Information operations exploit the technical nature of legal disputes to obscure responsibility. Cyber and electromagnetic interference occur within a context where jurisdiction over infrastructure and spectrum is contested. Together, these interactions demonstrate that legal ambiguity is not an isolated condition but a central enabling mechanism for hybrid coercion (Kittrie, 2016).

From an analytical perspective, the Georgian case illustrates how law can be weaponised through its absence as much as through its application. By preventing resolution while enforcing de facto control, Russia transforms uncertainty into leverage. The longer non-resolution persists, the more governance adapts around it, and the harder reversal becomes. Time functions as a coercive multiplier, converting temporary ambiguity into permanent constraint.

This dynamic is critical for understanding the broader European hybrid environment. Legal indeterminacy is not unique to Georgia, but Georgia shows how it functions when sustained over time and insulated from decisive enforcement. The case demonstrates that unresolved legal status is not merely

a diplomatic failure. It is a strategic condition that can be actively cultivated to impose continuous pressure while preserving plausible deniability and limiting escalation.

5.4. Electromagnetic Pressure and GPS Interference as Hybrid Coercion

Electromagnetic interference, particularly involving Global Navigation Satellite Systems, constitutes a critical but often under-analysed component of Russian hybrid coercion in Georgia. Unlike kinetic or territorial practices, electromagnetic pressure operates through technically ambiguous effects that are difficult to attribute conclusively yet impose immediate safety, regulatory, and administrative consequences. In the Georgian context, such interference reveals how Russia exploits civilian safety regimes and spectrum governance to generate disproportionate institutional disruption without engaging in overt hostilities.

Georgia's geographic proximity to Russian-controlled territories in Abkhazia and South Ossetia places it within range of Russian electronic warfare capabilities deployed in these areas. Russian military doctrine treats control and contestation of the electromagnetic spectrum as a core element of modern operations, integrating electronic warfare units with broader strategic objectives. Analysts note that Russian forces routinely deploy jamming and spoofing capabilities not only for battlefield advantage but also to shape the civilian operating environment in contested regions (Adamsky, 2015).

Georgia's proximity to Russian-controlled territories and the wider Black Sea interference environment makes GNSS disruption a strategically relevant concern. While incident documentation and attribution remain uneven, technical attribution is inherently complex. Open-source reporting on Russian-linked GPS spoofing shows how such disruption can affect civilian navigation while leaving responsibility contested, allowing the source to deny intent while still achieving operational effect (Burgess, 2019; Schmitt, 2017).

The coercive impact of GPS interference lies not in physical damage but in the activation of safety and compliance regimes. Civil aviation authorities are obligated to prioritise passenger safety above all else. Even brief or intermittent GNSS anomalies compel the issuance of notices, rerouting of flights, grounding of aircraft, and increased reliance on alternative navigation methods. Each of these responses generates cost, delay, and reputational risk for aviation authorities and carriers. These burdens fall entirely on civilian institutions and commercial operators rather than on the actor generating the interference.

Maritime navigation experiences similar effects. GNSS interference along the Black Sea affects commercial shipping, port operations, and coastal safety systems. Maritime authorities must issue warnings, adjust routing, and increase monitoring. These measures impose operational friction on trade and logistics while remaining difficult to classify as hostile acts. Spectrum interference therefore exploits safety-driven governance: institutions must respond conservatively even when intent and attribution remain uncertain (Bueger & Edmunds, 2017).

From a governance perspective, electromagnetic interference functions as a procedural disruptor. Regulatory frameworks governing aviation and maritime safety require action even when causality is uncertain. This creates a structural asymmetry. Russia can impose recurring costs with minimal effort, while Georgian authorities must repeatedly activate resource-intensive safety and verification processes. Over time, this contributes to administrative fatigue and heightened perceptions of vulnerability.

Electromagnetic pressure also interacts with legal indeterminacy. Spectrum governance is governed by international norms that are poorly equipped to address deliberate interference in grey-zone contexts. Complaints and reports can be filed, but enforcement mechanisms are weak and slow. This mirrors the broader legal vacuum surrounding Georgia's occupied territories, reinforcing the sense that disruption is actionable but not punishable (Schmitt, 2017).

Information effects further amplify the impact. GNSS disruptions generate public concern, particularly when aviation safety is implicated. Russian and proxy narratives routinely frame such incidents as technical malfunctions, environmental anomalies, or unrelated failures, deflecting attention from intentional interference. Georgian authorities, constrained by evidentiary uncertainty and diplomatic caution, often communicate conservatively, reinforcing ambiguity rather than resolving it. This communication gap contributes to erosion of public confidence in institutional control (Bennett & Livingston, 2018).

Electromagnetic interference in Georgia does not operate in isolation. It reinforces other coercive mechanisms by demonstrating the reach and persistence of Russian capabilities. Border communities experience territorial encroachment. State institutions manage legal ambiguity. Cyber operations disrupt information systems. Electromagnetic pressure adds a further layer by exposing vulnerabilities in everyday civilian infrastructure, reminding both institutions and populations that disruption can occur without warning or clear attribution (Mazarr, 2015).

From an analytical standpoint, the Georgian case illustrates how electromagnetic coercion functions as a low-visibility, high-impact tool within a broader hybrid strategy. It requires no permanent presence, leaves little physical trace, and exploits the responding system's own safety and regulatory obligations. Over time, repeated interference conditions institutions to expect disruption and to allocate resources defensively, diverting attention from long-term strategic priorities.

This dynamic has clear implications beyond Georgia. Similar patterns of GNSS interference have been observed elsewhere in Europe, but typically in episodic form. Georgia's sustained exposure demonstrates how electromagnetic pressure can be normalised as a background condition, reducing its perceived exceptionalism while preserving its coercive value. In this sense, Georgia again functions as an early-warning environment, revealing how spectrum-based coercion can migrate and scale across regions under conditions of ambiguity and constrained deterrence (Burgess, 2019; Schmitt, 2017).

5.5. Cyber Operations as Strategic Reinforcement within Hybrid Coercion

Cyber operations occupy a distinctive position within Russia's hybrid coercion strategy in Georgia because they function less as independent instruments of disruption and more as strategic reinforcement mechanisms that amplify pressure generated in other domains. Rather than seeking permanent degradation of digital infrastructure, Russian cyber activity in Georgia has been calibrated to impose episodic but politically salient disruption, reinforce perceptions of vulnerability, and signal the persistence of coercive capacity across domains.

Georgia has been subjected to repeated cyber campaigns attributed by Western governments to Russian state actors, most notably the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). These campaigns have targeted a broad range of institutions, including central government ministries, courts, electoral bodies, media organisations, and critical public services. Attribution by the United Kingdom explicitly identified Russian military intelligence as responsible for a coordinated cyber campaign against Georgia, describing the activity as part of a broader pattern of hostile state behaviour intended to undermine sovereignty and democratic governance (UK Foreign and Commonwealth Office, 2020).

The timing of these cyber operations is analytically significant. Rather than occurring randomly, major cyber incidents have coincided with moments of heightened political sensitivity, including national elections, constitutional debates, and periods of intensified engagement with Euro-Atlantic institutions. This temporal alignment indicates strategic intent. Cyber disruption is deployed to complicate governance precisely when institutional coherence, public trust, and administrative capacity are most critical. Scholars analysing Russian cyber doctrine emphasise that such timing reflects an understanding of cyber operations as instruments of political effect rather than purely technical tools (Connell and Vogler, 2017).

The operational characteristics of these campaigns further reinforce this interpretation. Attacks have frequently involved defacement, data disruption, denial of service, and interference with public communication platforms. While these methods rarely produce long-term technical damage, they generate immediate visibility and symbolic impact. Courts unable to publish decisions, ministries forced offline, and media outlets disrupted during critical news cycles undermine confidence in institutional competence. Consistent with Rid's account of active measures as disruption-oriented rather than purely destructive, the objective is temporary paralysis that magnifies uncertainty and reputational damage (Rid, 2020).

Cyber operations also interact directly with legal and administrative processes. Disruption of court systems and government databases delays legal proceedings, procurement decisions, and regulatory action. This reinforces the time-based coercion produced by legal indeterminacy and litigation pressure. Institutions must divert resources to incident response, forensic investigation, and system restoration, often under conditions of public scrutiny. These responses are costly and procedurally demanding, yet they rarely yield opportunities for counteraction against the source of interference (Lewis, 2020).

Cyber activity in Georgia has consistently been framed by Russian authorities and aligned media as criminal, technical, or unrelated incidents. This narrative strategy mirrors the ambiguity cultivated in physical and electromagnetic domains. Georgian authorities, constrained by evidentiary standards and diplomatic caution, typically communicate conservatively about attribution. This asymmetry allows Russia to benefit from disruption while avoiding immediate political cost. The result is a familiar hybrid dynamic in which responsibility is diffuse, but impact is concentrated (Galeotti, 2016).

From an institutional perspective, repeated cyber incidents contribute to adaptive fatigue. Georgian agencies develop response protocols and contingency plans, but the constant need for readiness diverts attention from strategic reform and long-term planning. Over time, cyber disruption becomes anticipated rather than exceptional, reinforcing the normalisation of vulnerability. This is a critical outcome of hybrid coercion. Once institutions internalise disruption as routine, the coercive actor can sustain pressure with relatively low additional effort (Mazarr, 2015).

Cyber operations also reinforce the psychological dimension of coercion. Visible attacks on state institutions communicate reach and persistence. They demonstrate that Russian capabilities extend beyond territorial control into the digital heart of governance. For a state like Georgia, where institutional legitimacy is closely tied to perceptions of modernity and administrative competence, such signals carry particular weight. Analysts note that cyber coercion is especially effective in environments where symbolic disruption undermines broader narratives of state capacity and alignment with Western norms (Pomerantsev, 2019).

Crucially, cyber operations do not operate in isolation. In Georgia, they are embedded within a broader system of coercion that includes borderisation, legal ambiguity, electromagnetic interference, and information pressure. Cyber activity amplifies the effects of these mechanisms by increasing uncertainty, consuming administrative bandwidth, and reinforcing perceptions of systemic exposure. This integration demonstrates why cyber operations should be analysed not as standalone threats, but as reinforcing elements within a hybrid strategy (Hoffman, 2007).

The Georgian case therefore illustrates how cyber operations function most effectively when they are subordinate to strategic objectives rather than dominant. Russia’s use of cyber coercion in Georgia shows that limited, well-timed disruption can produce enduring political and institutional effects when combined with pressure in other domains. This insight is essential for understanding the broader European hybrid environment, where similar cyber tactics are increasingly observed in conjunction with physical and legal forms of coercion (Kofman, Fink, and Edmonds, 2020).

5.6. Information Operations and Narrative Management as Institutional Coercion

Information operations constitute a central pillar of Russian hybrid coercion in Georgia, but their strategic function extends well beyond the dissemination of false narratives or propaganda. In the Georgian context, Russian information activity operates primarily as a mechanism of institutional coercion, designed to erode the authority, credibility, and decisional capacity of the state during moments when

public trust and compliance are most critical. The objective is not mass persuasion in a narrow sense, but the systematic degradation of the informational conditions under which governance operates.

Russian information operations in Georgia are characterised by selective amplification, narrative framing, and timing, rather than by constant message saturation. Content is injected into the information environment during periods of heightened stress, including border incidents, civilian detentions, cyber disruptions, elections, and moments of diplomatic engagement with Euro-Atlantic institutions. This timing is deliberate. It ensures that information pressure coincides with institutional vulnerability, magnifying the effects of physical, legal, and cyber coercion (European External Action Service, 2023).

A defining feature of this activity is the use of administrative mimicry. Russian and proxy actors frequently circulate messages that imitate official Georgian communications in tone, format, and terminology. Forged advisories, selectively edited official statements, and misleading translations are disseminated through social media, messaging platforms, and fringe media outlets. These materials do not always present overtly false claims. Instead, they introduce ambiguity about authenticity, authorship, and intent. Bennett and Livingston's framework supports the view that such practices undermine the credibility of authoritative sources rather than simply promoting alternative truths (Bennett and Livingston, 2018).

Minority-language communities are particularly vulnerable. Georgian state communication capacity is uneven across linguistic groups, and official translations can lag behind events. Russian messaging exploits these gaps by providing rapid, authoritative-sounding content in Russian, Armenian, and Azerbaijani (Minesashvili, 2020). This creates asymmetries in information access and verification. Residents may receive guidance and interpretation faster from unofficial sources than from the state, undermining trust even in the absence of explicit disinformation (European External Action Service, 2023; Pomerantsev and Weiss, 2014).

Information operations also exploit legal and institutional constraints on state speech. Georgian authorities are bound by evidentiary standards, diplomatic considerations, and legal obligations when communicating about incidents involving Russia. Attribution must be cautious (Janiashvili, 2023). Language must be precise. This caution creates informational vacuums during crises. Russian messaging fills these vacuums with narratives that frame incidents as misunderstandings, technical failures, or provocations by Georgian actors. The burden of proof is thereby shifted onto the weaker party, forcing restraint to be interpreted as uncertainty or guilt.

Narrative framing consistently emphasises inevitability and normalisation. Borderisation is presented as administrative reality. Detentions are framed as routine law enforcement. Cyber incidents are depicted as criminal acts or technical malfunctions. GPS interference is explained away as an environmental anomaly. Over time, this framing conditions audiences to view coercive practices as background conditions rather than violations requiring response. The most important effect is therefore habituation, not outrage (Janiashvili, 2023; Pomerantsev & Weiss, 2014; Bennett & Livingston, 2018).

From an institutional perspective, information operations impose significant governance costs. Public officials must devote time and resources to verification, clarification, and correction. Messaging is delayed while legal and diplomatic review occurs. Conflicting narratives reduce public compliance with official guidance, particularly during crises involving safety or infrastructure. This creates a feedback loop in which hesitation breeds mistrust, further weakening authority (Bennett & Livingston, 2018; Freelon & Wells, 2020).

Information operations also interact with cyber and electromagnetic coercion. Cyber disruptions to government websites and media outlets reduce the state's capacity to communicate authoritatively. GPS interference generates safety concerns that demand rapid public guidance. When these pressures coincide with information manipulation, institutional communication capacity is degraded precisely when it is most needed. The cumulative effect is systemic rather than episodic (Starbird et al., 2019).

Russian information operations in Georgia do not aim to wholesale replace Georgian narratives with Russian ones. Instead, they seek to fragment the informational environment, multiplying competing interpretations and eroding the expectation that any single source is authoritative. This fragmentation reduces the political cost of continued coercion by lowering public expectations of clarity or resolution; in effect, confusion becomes a stabilising condition for the coercer.

The Georgian case demonstrates that information operations function most effectively when embedded within a broader coercive system. Physical encroachment creates incidents. Legal ambiguity constrains response. Cyber and electromagnetic interference degrade capacity. Information pressure ensures that these dynamics are perceived as normal, ambiguous, and unavoidable. Together, they illustrate how narrative management operates not as persuasion, but as institutional attrition.

This insight has broader relevance beyond Georgia. Similar information dynamics are increasingly visible elsewhere in Europe, particularly during infrastructure disruptions, elections, and legal disputes involving Russia. Georgia's sustained exposure reveals how information operations evolve over time from acute manipulation into structural features of governance stress. Understanding this evolution is essential for interpreting hybrid coercion as a long-term condition rather than a series of discrete influence campaigns (Bennett & Livingston, 2018).

5.7. Georgia as an Early-Warning Environment for Hybrid Coercion in Europe

Georgia's value as an early-warning environment lies in the continuity and visibility of Russian coercive practice under conditions of weak deterrence. Border adjustments, detentions, cyber disruption, electromagnetic interference, and information pressure recur often enough to show how micro-events accumulate into durable governance constraints.

Because Georgia lacks the alliance guarantees and crisis-management depth available to NATO members, institutions absorb these pressures directly. Their adaptation reveals a key risk for Europe: resilience can become routinisation when repeated exposure improves handling but lowers expectations of reversal.

The results presented above reinforce and extend existing scholarship on hybrid coercion by demonstrating that its primary strategic value lies not in tactical novelty, but in its capacity to reconfigure governance itself as a site of contestation. Rather than operating at the margins of security policy, hybrid coercion penetrates the administrative, legal, and informational routines that sustain state authority in democratic systems. This finding aligns with prior work that conceptualises hybrid conflict as a condition of continuous competition rather than episodic confrontation, but the present analysis advances this literature by showing how that competition is operationalised through procedural dependence rather than persuasion or force alone.

Existing scholarship has often treated individual hybrid tactics in isolation, focusing separately on cyber operations, disinformation, legal warfare, or infrastructure security. The findings here suggest that such compartmentalisation obscures the central dynamic of hybrid coercion, which is cross-domain reinforcement over time. Physical disruption, legal ambiguity, electromagnetic interference, cyber activity, and information operations do not merely co-occur. They interact in ways that systematically constrain institutional choice, forcing authorities into conservative, delayed, and fragmented responses. This interaction supports theoretical claims that hybrid coercion should be analysed as a system rather than a toolkit, but it also specifies the mechanisms through which systemic effects are produced.

The Georgian case complicates assumptions in the literature regarding deterrence and resilience. Much of the existing research assumes that exposure to hybrid threats leads to institutional learning and adaptation that strengthens resilience over time. The findings here suggest a more ambivalent dynamic. While Georgian institutions have undoubtedly improved technical response capacity, the dominant adaptive outcome has been administrative normalisation rather than strategic resolution. Repeated exposure has reduced surprise and improved crisis handling, but it has also lowered expectations of reversal and embedded coercion into routine governance. This raises important questions about whether resilience, as currently conceptualised, risks becoming a stabilising condition for coercion rather than a pathway to its mitigation.

The analysis also contributes to debates on attribution and escalation. Prevailing policy discourse often treats attribution as the primary barrier to effective response. While attribution challenges are significant, the findings indicate that even when responsibility is widely understood, institutional response remains constrained by legal standards, safety regimes, and political risk. Hybrid coercion succeeds not because attribution fails entirely, but because attribution alone does not unlock proportionate countermeasures within existing governance frameworks. This insight suggests that deterrence strategies focused narrowly on attribution may underestimate the structural sources of vulnerability.

Georgia’s role as an early-warning environment has broader implications for European security governance. The Georgian case demonstrates how hybrid coercion matures when ambiguity is sustained over long periods and enforcement mechanisms remain weak. The migration of similar tactics Westward suggests that what appears as episodic disruption in larger European states may represent early phases of a longer coercive cycle rather than isolated incidents. This challenges the tendency to treat hybrid activity as exceptional or crisis-bound and instead frames it as an enduring condition that requires institutional, legal, and procedural adaptation.

Finally, the findings underscore the need to rethink the relationship between law, legitimacy, and security. Hybrid coercion exploits the normative strengths of democratic governance by converting legality, due process, and transparency into sources of delay and constraint. This does not imply that these norms should be abandoned. Rather, it suggests that legal and regulatory systems must be recalibrated to operate under conditions of sustained ambiguity. Future research should therefore focus not only on identifying hybrid threats, but on designing governance mechanisms capable of acting decisively without forfeiting legitimacy.

Taken together, the discussion indicates that hybrid coercion is best understood not as a failure of deterrence or communication, but as a strategic exploitation of how democratic systems are designed to function. Georgia reveals what happens when such exploitation is allowed to persist over time. The challenge for Europe is to draw lessons from this exposure before episodic pressure hardens into structural constraint.

6. Conclusion

This article has argued that Russia's hybrid coercion in Europe operates not as a collection of isolated tactics, but as an integrated system designed to impose sustained governance pressure across physical, legal, informational, cyber, and electromagnetic domains. Its effectiveness derives less from disruption alone than from the cumulative institutional effects generated when democratic systems must respond under ambiguity.

Georgia shows how this system functions when deterrence is limited and ambiguity persists over time. Borderisation, legal indeterminacy, spectrum interference, cyber operations, and narrative management interact to normalise uncertainty and embed coercion into routine governance without requiring escalation to armed conflict.

The policy implication is that deterrence and resilience must be procedural as well as declaratory. Effective responses require faster attribution pathways, pre-agreed response thresholds, coordinated legal and regulatory playbooks, and crisis communication systems capable of acting decisively without forfeiting legitimacy. Recognising this transformation is essential before episodic pressure hardens into structural constraint elsewhere in Europe.

The statement regarding the usage of AI: Artificial intelligence (AI) tools were used solely for language editing, stylistic refinement, and improving the clarity and readability of the manuscript. Specifically, OpenAI's ChatGPT was utilized to assist with grammar correction, sentence structure improvement, and enhancement of academic writing style. The authors reviewed, verified, and take full responsibility for all content, interpretations, analyses, and conclusions presented in this article.

Funding: This research has received no external funding.

Conflict of Interests: The author declares no conflict of interest regarding this study.

References

1. Adamsky, D. (2015). *Cross-Domain Coercion: The Current Russian Art of Strategy*. Institut Français des Relations Internationales.
2. Alter, K. J. (2014). *The New Terrain of International Law: Courts, Politics, Rights*. Princeton University Press.
3. Bahenský, V., Daniel, J., & Turcsányi, R. Q. (2023). *Dragon's Roar and Bear's Howl: Convergence in Sino-Russian Information Operations in NATO Countries?* NATO Strategic Communications Centre of Excellence.
4. Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.
5. Bennett, W. L., & Livingston, S. (2018). "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions." *European Journal of Communication*, 33(2), 122–139. https://doi.org/10.1177/0267323118760317
6. Bescotti, E. (2019). "A Non-Resolution Limbo: Better Status Quo than Settled? Georgian Territorial Integrity, Russian Security Interests, and the Status of De Facto States in the Peace Process," in OSCE Yearbook 2019 (Baden-Baden: Nomos, 2020), 151–161.
7. Boyle, E. (2017). "Borderization in Georgia: Sovereignty Materialized." *Eurasia Border Review*, 7(1), 1–18. https://doi.org/10.14943/ebr.7.1.1
8. Bueger, C., & Edmunds, T. (2017). "Beyond Seablindness: A New Agenda for Maritime Security Studies." *International Affairs*, 93(6), 1293–1311. https://doi.org/10.1093/ia/iix174
9. Burgess, M. (2019, March 26). "To Protect Putin, Russia Is Spoofing GPS Signals on a Massive Scale." *Wired*. Retrieved from www.wired.com
10. Cappella, J. N., & Jamieson, K. H. (1997). *Spiral of Cynicism: The Press and the Public Good*. Oxford University Press.
11. Connell, M., & Vogler, S. (2017). *Russia's Approach to Cyber Warfare*. CNA.
12. De Waal, T. (2018). *Uncertain Ground: Engaging with Europe's De Facto States and Contested Territories.* Carnegie Europe. Retrieved from www.carnegieendowment.org
13. Eggen, K.-A., & Lavikainen, J. (2025). "Implementing a New Tool: Russia's Strategic Use of Migrants towards Norway and Finland 2015/16." *European Journal of International Security*, FirstView, 1–24. https://doi.org/10.1017/eis.2025.10029
14. European External Action Service. (2026). Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). European Union. Retrieved from www.eeas.europa.eu
15. European External Action Service. (2023). 1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence. European Union. Retrieved from www.eeas.europa.eu

16. European Union. (2022). "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union." *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/
17. Farrell, H., & Newman, A. L. (2019). "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security*, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351
18. Freelon, D., & Wells, C. (2020). "Disinformation as Political Communication." *Political Communication*, 37(2), 145–156. https://doi.org/10.1080/10584609.2020.1723755
19. Fridman, O. (2017). "Hybrid Warfare or Gibridnaya Voyna?" *The RUSI Journal*, 162(1), 42–49. https://doi.org/10.1080/03071847.2016.1253370
20. Galeotti, M. (2016). "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?" *Small Wars & Insurgencies*, 27(2), 282–301. https://doi.org/10.1080/09592318.2015.1129170
21. George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*. MIT Press.
22. Giles, K. (2016). *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. Chatham House.
23. Goldthau, A., & Sitter, N. (2015). *A Liberal Actor in a Realist World: The European Union Regulatory State and the Global Political Economy of Energy*. Oxford University Press.
24. Helfer, L. R., & Alter, K. J. (2013). "Legitimacy and Lawmaking: A Tale of Three International Courts." *American Journal of International Law*, 107(3), 479–530. https://doi.org/10.5305/amerjintelaw.107.3.0479
25. Hellström, J., Kallioniemi, P., Kytöneva, S., & Puranen, M. (2024). *Are Russian Narratives Amplified by PRC Media?* NATO Strategic Communications Centre of Excellence.
26. Hoorman, C., & Vincent, E. (2024, December 28). "How NATO Is Organizing to Protect Submarine Cables after Series of Incidents." *Le Monde*. Retrieved from www.lemonde.fr
27. Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies. Retrieved from www.comw.org
28. Jamieson, K. H., & Cappella, J. N. (2008). *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment*. Oxford University Press.
29. Janiashvili, E. (2023). "Russian Information Operation in the South Caucasus: Accounts Operating in Social Networks and Their Messages." *International Society for Fair Elections and Democracy*. Retrieved from www.isfed.ge
30. Kelmendi, T., and Kapanadze, S. (2025). "Occupational Therapy: Frozen Conflicts, Russian Aggression and EU Enlargement." *European Council on Foreign Relations*. Retrieved from www.ecfr.eu
31. Kittrie, O. F. (2016). *Lawfare: Law as a Weapon of War*. Oxford University Press.

32. Kofman, M., Fink, A., & Edmonds, J. (2020). *Russian Strategy for Escalation Management: Evolution of Key Concepts*. CNA. Retrieved from www.cna.org
33. Lanoszka, A. (2016). "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe." *International Affairs*, 92(1), 175–195. https://doi.org/10.1111/1468-2346.12509
34. Lanoszka, A. (2018). "Stop Calling Every Potential Act of Russian Aggression 'Hybrid Warfare.'" *International Affairs Blog*. Retrieved from www.medium.com
35. Lewis, J. A. (2020). *Cybersecurity and Critical Infrastructure Protection*. Center for Strategic and International Studies.
36. March, J. G., & Olsen, J. P. (1989). *Rediscovering Institutions*. Free Press.
37. Mazarr, M. J. (2015). *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. U.S. Army War College Press.
38. Minesashvili, S. (2020). "EU and Ethnic Minorities in Georgia: How to Counter Misinformation and Disruptive Communication." Policy Brief no. 29. *Georgian Institute of Politics*. Retrieved from www.gip.ge
39. Monaghan, A. (2019). *Power in Modern Russia: Strategy and Mobilisation*. Manchester University Press.
40. Monaghan, S., Svendsen, O., Darrah, M., & Arnold, E. (2023). *NATO's Role in Protecting Critical Undersea Infrastructure*. Center for Strategic and International Studies. Retrieved from www.jstor.org
41. Morgan, F. E., Bender, J., Cragin, K., Massicot, D., & Tellis, A. J. (2019). *Competing in the Gray Zone: A Strategy to Counter Russian and Iranian Gray Zone Aggression*. RAND Corporation.
42. Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It.* RAND Corporation. Retrieved from www.rand.org
43. Polyakova, A., & Meserole, C. (2019). *Exporting Digital Authoritarianism: The Russian and Chinese Models*. Brookings Institution.
44. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War against Reality*. Faber & Faber.
45. Pomerantsev, P., & Weiss, M. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Interpreter / Institute of Modern Russia. Retrieved from www.interpretermag.com
46. Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.
47. Rolland, N. (2020). *China's Vision for a New World Order*. National Bureau of Asian Research.

48. Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
49. Seaman, J., Huotari, M., & Otero-Iglesias, M. (Eds.). (2021). *Chinese Economic Statecraft: Lessons for Europe*. European Think-Tank Network on China.
50. Starbird, K., Arif, A., & Wilson, T. (2019). "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations." *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), Article 127. https://doi.org/10.1145/3359229
51. UK Foreign and Commonwealth Office. (2020). *UK Condemns Russia's GRU over Georgia Cyber-Attacks*. UK Government. Retrieved from www.gov.uk
52. U.S. Department of Justice. (2024). "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere." Retrieved from www.justice.gov
53. Weiss, M., Dobrokhotov, R., & Grozev, C. (2024). "Unraveling Havana Syndrome: New Evidence Links the GRU's Assassination Unit 29155 to Mysterious Attacks on U.S. Officials and Their Families." *The Insider*. Retrieved from www.theins.press
54. Wither, J. K. (2016). "Making Sense of Hybrid Warfare." *Connections*, 15(2), 73–87. https://doi.org/10.11610/Connections.15.2.06