

Report



Europe's Moment of Truth

A Democracy Shield for Today
and Tomorrow

Vassilis Ntousas and Etienne Soula

G | M | F

Alliance for
Securing
Democracy

Executive Summary

Democracy in Europe is under growing pressure. Authoritarian regimes like Russia and the People's Republic of China are conducting increasingly sophisticated foreign interference campaigns that blend information manipulation, cyberattacks, malign finance, economic coercion, and kinetic operations. Internally, illiberal actors are eroding the rule of law and civic freedoms as democratic norms deteriorate in the EU's immediate neighborhood. The EU's current response often remains fragmented and reactive, exposing it to external interference and internal backsliding.

The European Democracy Shield, announced in 2024 and expected in 2025, presents a unique opportunity to consolidate democratic defense. If designed as more than a symbolic initiative, the Shield can equip the EU with a credible, coordinated, and enforceable framework to safeguard democratic integrity at home and project protection outward.

The aim of this report is to support the development of an effective and resilient European Democracy Shield. To this end, Part 1 maps the **current threat landscape**, highlighting the main challenges to democratic systems across the EU. Part 2 **identifies key institutional and policy gaps** that limit the EU's capacity to respond to these threats. Part 3 sets out **ten actionable recommendations** designed to ensure the Shield is not only politically resonant but also operationally impactful. These are:

1. **See the forest:** Treat authoritarian interference as a longitudinal threat and forge an integrated, cross-domain response.
2. **Standardize language to strengthen strategy:** Adopt clear and consistent terminology across institutions to support unified strategy and action.
3. **Enhance situational awareness:** Build a real-time "Democracy Radar" combining EU-wide monitoring, foresight, and national-threat reporting.
4. **Maximize enforcement of existing tools:** Fully implement and coordinate use of existing tools, most notably the Digital Services Act.
5. **Preserve information integrity:** Address the financial and regulatory drivers of manipulation and reinforce safeguards around elections.
6. **Reinforce national democratic foundations:** Link EU support to democratic reform and institutional capacity-building across member states.
7. **Develop national anti-foreign information manipulation and interference defenses:** Ensure each member state has processes or institutions dedicated to the detection of, and response to, interference.

8. **Elevate the defender network:** Recognize and protect the foundational role for civil society, media, and citizens in democracy protection.
9. **Invest in core support for democratic resilience:** Move from short-term grants to strategic, long-term support for core democratic functions.
10. **Project protection outward:** Support partner democracies with adaptable tools and deepen democratic cooperation globally.

Taken together, these steps would transform the Shield into a strategic, whole-of-Union response to both external and internal challenges while positioning Europe as a global leader in demonstrating how democracy can be safeguarded by design, today and tomorrow.

Introduction

Democracy in Europe is under siege. Revisionist powers like Russia and the People's Republic of China (PRC) are combining tools and tactics like information manipulation, cyber warfare, malign finance, economic coercion, and societal subversion into sustained campaigns aimed at destabilizing democratic systems. Hybrid warfare compounds these threats, from orchestrated border crises and supply-chain disruption to the infiltration of organized crime networks and kinetic operations, contributing to a broader sense of insecurity. In addition, the erosion of democracy is not just an external threat. Within the EU, illiberal actors are undermining judicial independence, media freedom, and democratic accountability. Democratic norms are also retreating in Europe's backyard, where countries in the Western Balkans and Eastern Partnership bloc are increasingly serving as testing grounds for anti-democratic tactics.

Europe's existing policies and regulatory frameworks have struggled to keep pace with the complexity of this all-out assault on its democratic infrastructure. This has left the EU vulnerable to both foreign interference and internal democratic erosion. The European Democracy Shield (EUDS), first announced by Commission President Ursula von der Leyen in 2024 and expected to be unveiled in late 2025, represents a singular opportunity to move beyond fragmented responses and create a coherent, long-term defense of European democracy. To be effective, the Shield must be more than symbolic. It must be strategic, enforceable, and forward-looking, designed to protect democratic systems inside the EU as well as beyond the bloc's borders.

This report aims to ensure that the EUDS becomes a meaningful and effective instrument for defending democracy. It is structured in three sections: the first maps the severe threat landscape that calls for a robust Shield; the second reviews the key actions already taken by the EU to date while highlighting persistent gaps in that approach; and the third presents ten actionable recommendations to help the Shield make a meaningful contribution to democratic defense. These recommendations adopt primarily a foreign interference-focused perspective. Collectively, they aim to ensure that the EUDS delivers a cohesive response rooted in European values, bolsters transparency and accountability, and is truly capable of confronting the challenges of today and tomorrow with clarity and strength.

Part 1 – A Shield Against What? Understanding the Interference Threat Landscape

As democracy faces mounting global pressure, the EU is being targeted by nefarious actors, both foreign and domestic. The EUDS, led by Commissioner Michael McGrath and overseen by Executive Vice-President Henna Virkkunen, is the EU's most ambitious initiative to date aimed at reinforcing democratic resilience and countering forces that seek to undermine it. But what exactly is the nature of the threat? This section maps the evolving interference landscape, highlighting the urgent need for a credible, coordinated, and comprehensive defense of democracy. It makes clear why a robust Shield is no longer optional, but essential.

Global Democratic Backsliding

The EUDS must be built with a clear-eyed understanding of the geopolitical reality in which it will operate. Around the world, democracy is under concerted assault. Authoritarian regimes are more confident and technologically sophisticated and increasingly coordinate with each other. Through far-reaching influence operations, they challenge liberal democracies domestically as well as across international fora. For Europe, this growing global pressure is a key part of the wider threat landscape that the Shield must be prepared to contend with.

Russia and the PRC stand at the heart of this [authoritarian surge](#). Their tactics differ, but their goals broadly align: to weaken democratic norms and isolate those who champion them, notably by sowing public distrust in open societies; and to reshape global institutions into venues that are more favorable to autocratic power. Russia's continued use of information manipulation and other tools of interference to meddle in elections and more broadly destabilize democratic societies is now a core feature of its foreign policy. Its efforts aim to create chaos abroad and justify the Kremlin's repression at home. Meanwhile the PRC relies on economic coercion, elite capture, and media control to advance a model of "stable" authoritarianism and export surveillance technologies to sympathetic regimes.

These tactics are having a global spillover effect. Across the world, authoritarian-leaning governments are studying and adapting elements of Russian and PRC foreign interference campaigns, blending digital repression with legal mechanisms and intimidation. This trend of authoritarian learning has helped to create a global network of actors who share tools and tactics, attempting to bend democratic rules, silence dissent, and resist accountability. In this environment of increasingly brazen authoritarianism, the EU must contend with adversaries who are better coordinated, more agile, and ever more confident.

This challenge is compounded by growing uncertainty around the future of democratic leadership globally. Fewer countries today appear willing and able to take a clear stand in defense of democratic principles. This hesitation has emboldened authoritarian states, encouraged fence-sitting by swing countries, and further fragmented the democratic front.

In such an environment, the absence of robust democratic defenses becomes not just a vulnerability, but an invitation to would-be attackers. The EU, one of the last actors with the credibility, capacity, and strategic interest to lead, must step up. The EUDS must therefore recognize three core imperatives: asserting the EU as a global ally to democratic reformers; treating democracy support as a strategic priority; and strengthening internal democratic integrity to credibly confront external threats.

A Neighborhood Under Pressure

Europe's neighborhood is a casualty of the global democratic backslide and has become a frontline where democracy is under sustained, organized assault. In countries like Ukraine, Georgia, Moldova, and across the Western Balkans, authoritarian actors are actively probing the resilience of democratic institutions. These actions are neither incidental nor opportunistic. They are systematic, strategic, and deliberately designed to constrict democratic space.

Russia remains the most aggressive player in this arena. Its war on Ukraine is not just a military campaign, but a direct attack on Europe's democratic identity, executed through a full-spectrum strategy that includes foreign information manipulation and interference (FIMI), hybrid tactics, and conventional force. In Moldova, Russia backs oligarchic networks, fuels illiberal sentiments, and amplifies anti-EU narratives to undermine pro-European forces.

The PRC is also steadily expanding its influence in the EU's neighborhood mainly through infrastructure investments, media penetration, and elite-level diplomacy, especially in the Western Balkans. In countries like Serbia, PRC and Russian interests often converge, fostering an authoritarian-friendly environment that tries to position liberal democracy as fragile and dispensable.

Yet the threat is not solely external. In several states, domestic political elites are adopting authoritarian tactics. Serbia's government has systematically attempted to hollow out democratic institutions through state capture and media control. In Georgia, the ruling party increasingly emulates Moscow's playbook, pushing repressive laws that echo Russia's approach to dissent. Even in more reform-oriented countries like Ukraine and Moldova, deep systemic vulnerabilities form an environment permeable to persistent corruption, hybrid threats, and to the constant threat of authoritarian violence.

In light of this, the EUDS presents a critical opportunity to push back against growing authoritarian influence in the EU's own neighborhood as well. While the Shield will not replace the broader efforts already underway beyond Europe's borders, ranging from its neighborhood policy to trade and development cooperation, it must elevate democracy from a boilerplate talking point to a core pillar of EU foreign and security policy. It also can and should help articulate a clearer, more strategic EU offer to its neighbors. This is not a peripheral concern, as those neighbors are Europe's first line of defense, with countries like Ukraine and Moldova giving EU members the opportunity to learn from the most extreme application of the FIMI and hybrid playbooks. Further cracks there will be a gateway for more authoritarian influence directly into the Union.

A Union at a Crossroads

Last but certainly not least, democracy is under siege inside the EU itself. Government of the people, for the people, and by the people is a direct target of sophisticated campaigns that blend different tactics from the FIMI toolkit with hybrid, kinetic, cyber and other attack elements to undermine the EU's information space, regulatory frameworks, political parties, critical infrastructure and services, as well as its democratic processes and institutions.

In the information space alone, threat actors such as Russia and the PRC deploy tactics that include the creation of large networks of fake news sites and inauthentic (bot) accounts, increasingly supercharged through the use of artificial intelligence (AI), to shape public opinion, drown out dissident voices, and weaken democratic cohesion. In the physical realm, kinetic operations [are also escalating](#), as seen in sabotage and arson attempts, parcel bombs, and the 2024 [assassination plot](#) against a senior defense-industry executive in Germany. These operations are often carried out through proxies, complicating attribution and maximizing disruption.

Other authoritarian powers have also joined the contest. In 2022, the '[Qatargate](#)' corruption scandal that saw foreign governments, including Qatar and Morocco, reportedly pay bribes to influence European Parliament decisions, laid bare how Russia and the PRC are not the only ones seeking to interfere in EU democracies. It illustrates a broader trend of external actors seeking to extend their influence onto and into the EU itself.

This evolving playbook is specifically designed to further polarize societies, delegitimize institutions, and paralyze decision-makers. Its effectiveness is amplified by structural vulnerabilities within the EU: at times inconsistent legal frameworks, spotty enforcement of existing laws, exploitable lobbying and financial rules, under-resourced national regulators, and a reliance that too often veers into dependance on a handful of powerful digital platforms with uneven interest in accountability. The digitalization of the information space, financial sector, and even critical infrastructure has expanded the attack surface available to malign actors.

Critically, though, the erosion of democratic norms is not solely driven by external threats. Across the EU, [domestic political actors](#) are increasingly adopting tactics once associated with foreign interference. These include the use of state resources and algorithmically amplified information manipulation to target opposition, attacks on independent media and civil society, as well as the weakening of the rule of law and judicial independence. In Hungary, and increasingly in other member states, ruling parties are mirroring the legal, policy, and rhetorical strategies of authoritarian regimes to restrict civic space and consolidate power. This convergence blurs the line between internal and external threats, making defense more difficult and politically sensitive.

The result is a dual pressure on EU democracy: an external campaign of destabilization complemented by internal degradation of democratic standards. Both trends reinforce each other, leaving institutions overstretched and citizens disillusioned.

The EUDS must provide an answer to this daunting challenge. It presents an opportunity to consolidate fragmented efforts and respond appropriately to the scale of the threat. It should provide a coherent framework that closes legal gaps, strengthens enforcement, enhances threat monitoring, and anchors democratic resilience at the center of European security. Anything less risks allowing these advanced, multi-domain campaigns to continue unchecked and further erode the Union's foundation.

Part 2 – A Shield Fixing What? Identifying the Gaps

European democracy faces an immediate, multifaceted, and intensifying assault. The Shield's announcement comes as an acknowledgement of this harsh geopolitical reality. However, for the EUDS to amount to more than a rhetorical gesture, it must directly confront the EU's systemic vulnerabilities. It must coordinate and harmonize fragmented initiatives, close critical legal and enforcement gaps, and establish a durable framework for strategic democratic defense. This section outlines several of the most pressing gaps that must be addressed.

At the **global** level, the EU has long positioned itself as a standard-setter, shaping international norms in domains vital to democracy such as the rule of law, data privacy, human rights, and electoral integrity. Through instruments that began in the previous Commission mandate, like [Global Gateway](#) and [NDICI-Global Europe](#), it supports governance, infrastructure, and development across what is commonly referred to as the Global South. Its [foreign policy](#) has consistently sought to promote democratic values through multilateral, plurilateral, and bilateral diplomacy. Yet this approach has too often underdelivered, a pattern likely to worsen as the geopolitical environment becomes increasingly contested. Indeed, as great-power competition exacerbates tensions between democratic and authoritarian models in the Global South, the EU's approach appears particularly inadequate. Europe's rules-based diplomacy often struggles to compete with the faster, opaque, and transactional offers made by authoritarian actors, particularly the PRC and Russia, whose strategies are largely unburdened by transparency or rights-based conditions.

Meanwhile, local democratic actors are often left without the necessary infrastructure, such as cybersecurity, legal protections, or strategic communications tools, to withstand pressure or repression. These external shortcomings are compounded by the global funding crunch affecting all democracy-affirming work. Furthermore, internal deficiencies within EU institutions and member states can also undermine the bloc's credibility.

The EUDS is not a silver bullet, but if properly designed, it can begin to fill this void. At the very least, it can send a clear signal that those defending democracy in today's world are not alone. It can help reignite the EU's own democratic ethos, clarify where and how the Union prioritizes democracy support, and align its geopolitical instruments with its democratic values, delivering timely and flexible aid, scaling up capacity-building, and reasserting leadership in the global contest over governance.

The Shield can also have a transformative impact at the **neighborhood** level, where key geopolitical partners and democratic allies face the dual pressures of internal fragility and external interference. To its credit, the EU has already developed a wide array of tools to support resilience in this space: an enlargement process that is intended to incentivize reform; concrete assistance to counter FIMI, cyber, and hybrid threats; diplomatic coordination on attribution of identified destabilization attempts; support for civil society and independent media; the work of the European External Action Service (EEAS) StratCom divisions; and the deployment of peace- and stability-fostering missions under the Common Security and Defense Policy. These efforts have been reinforced by strong references in key EU strategic documents, most notably the [Strategic Compass](#), which rightly frames the contest in the region

as a “competition of governance systems.” This reflects a growing awareness that the future of European security is inseparable from the democratic resilience of its immediate neighborhood.

Despite these initiatives, significant gaps remain in the EU's coherence and effectiveness in its near abroad. In an increasingly competitive regional environment, efforts are often siloed, under-resourced, or poorly coordinated. Democracy support and hybrid threat mitigation tend to operate in parallel, with limited integration. In some cases, such as [Ukraine](#), partner governments have experienced challenges in securing timely EU political and financial support during periods of heightened need. In others, such as [Serbia](#) and [Georgia](#), clear democratic backsliding has been met with modest EU pushback. The EU has developed a number of relevant toolboxes, including in [cyber diplomacy](#), yet they remain unevenly applied. Meanwhile, the EEAS StratCom divisions remain modestly staffed despite growing demand, and civil society support frequently depends on short-term funding cycles that hamper the development of long-term resilience. The enlargement process itself, and the political conditionality it entails, is in urgent need of reform. Without greater clarity, consistency, and credibility, the EU's offer to the region risks losing both traction and trust.

The Shield cannot solve all these challenges, particularly given its primarily inward-facing mandate. However, it would be a missed opportunity if it did not, by extension and design, help clarify and consolidate the EU's strategic offer to its neighborhood. The EUDS can serve as a unifying framework, bringing together democracy support, counter-interference tools, and foreign policy leverage into a single, coherent strategy. Above all, through the Shield, the EU must deepen its understanding of its neighborhood not as a buffer zone, but as a shared democratic space, one that is essential to its own stability and security.

Finally, turning to the **domestic** level, it is clear that while the EU has taken important steps to reinforce its democratic resilience, domestic assaults against norms and institutions and foreign interference operations have exposed its limited capacity to defend democracy within its own borders. In recent years, the EU has made significant progress in shifting from a reactive to a more anticipatory approach across the [FIMI](#) and [hybrid](#) domains. Institutional tools have expanded, including the establishment of the Rapid Alert System, the development of the Hybrid Fusion Cell within the EEAS, and the ongoing work of the StratCom divisions, all of which have improved the EU's ability to monitor, attribute, and respond to interference campaigns.

On the legislative front, the [Digital Services Act](#) (DSA) introduces systemic risk obligations for major platforms, aiming to curb information and algorithmic manipulation, while the [AI Act](#) establishes safeguards against the political misuse of AI, including deepfakes and microtargeting. Additional initiatives such as the [European Democracy Action Plan](#), the [Defense of Democracy package](#), and the [Political Advertising Regulation](#) further demonstrate the EU's growing recognition that defending democracy requires proactive protection from malign influence.

This evolving architecture is supported by a more coherent and shared threat assessment. Just within the FIMI domain, key strategic documents, including the [Strategic Compass](#) and the EEAS [reports on FIMI threats](#), explicitly identify state-sponsored interference, particularly from Russia and the PRC, as a systemic threat to European security and democratic sovereignty. The [2024 Niinistö Report](#) further reinforced this framing, calling for stronger institutional leadership, improved cross-sectoral coordination, and more decisive action to counter hybrid threats. Political and

institutional momentum has also increased. Successive European Council conclusions have acknowledged the seriousness of [FIMI](#) and [hybrid](#) campaigns, calling for enhanced coordination and resilience. Internally, the EU has shown a growing willingness to act, activating Article 7 proceedings for rule of law violations, and linking EU funding to democratic performance through the Rule of Law Conditionality regulation, including the temporary [suspension](#) of cohesion funds. Together, these developments represent a maturing response to threats to democracy, one that increasingly bridges the external and internal dimensions of authoritarian interference.

Still, substantial gaps remain. The FIMI domain offers a clear example. Indeed, while threats to democracy are multiplying, the EEAS' latest FIMI threat report [pointed out](#) the need to "move towards anticipatory analysis", implying that Europe's current monitoring capabilities often remain reactive. At the national level, few countries have adopted dedicated strategies or processes to counter FIMI, and even fewer, such as France and Sweden, have established specialized agencies to lead this effort. Meanwhile, Europe's civil society ecosystem has been severely affected by the global defunding of this field, particularly following cuts in US support. As a result, efforts to better coordinate and strengthen the anti-FIMI community continue to face several challenges: the uneven readiness of national authorities to address the threat, delays in the adoption and dissemination of standardized taxonomies—like the [ABCDE Framework](#), catalogues of threat actors' Tactics, Techniques, and Procedures, and [Structured Threat Information Expression](#) data-sharing formats—and the ongoing struggle of the expert community to sustain vital work often under adverse financial and political conditions.

A core obstacle lies in the disconnect between how the EU approaches foreign interference and how it responds to internal democratic backsliding. While the EU has developed an expanding toolbox for countering FIMI, ranging from regulation to strategic communications and attribution, domestic threats are addressed through entirely separate legal and political channels. Yet in practice, both foreign and domestic actors exploit similar tactics: information manipulation, malign finance, and civil society subversion. The rigidity of this bifurcation, resulting in institutional siloing, undermines operational coherence and weakens the credibility of democratic defense. Similarly, FIMI operations, cyberattacks, hybrid operations, and kinetic disruptions are still often treated in isolation, even though adversaries fluidly combine them to exploit cross-domain vulnerabilities. As a result, the specialized toolkits developed by the EU in cyber diplomacy, hybrid response, and FIMI—while strong and necessary on their own merits—show significant room for improvement in their coordination.

Conceptual inconsistency further hampers progress. The term "FIMI", introduced by the EEAS, understandably separates foreign and domestic domains in line with its creator's mandate but, on the ground, these boundaries are far less clear. Domestic actors increasingly adopt the same methods as foreign agents, either acting as witting or unwitting proxies or mimicking authoritarian tactics to entrench their own power. EU terminology only deepens the ambiguity: disinformation is sometimes treated as a subset of FIMI, sometimes as a standalone threat, and hybrid threats may include or exclude FIMI, kinetic aggression, or economic coercion. The picture becomes even more blurred when cyber risks are added. This lack of conceptual clarity undermines unified threat recognition and hinders cross-sectoral responses.

Legal and regulatory frameworks pose further challenges. Although the DSA and AI Act represent major advances, their enforcement remains uneven and slow. National regulators often lack sufficient resources and expertise,

resulting in widely inconsistent implementation across the bloc. Algorithmic manipulation, as well as deepfakes and other AI-powered tools exploited by nefarious actors to conduct information manipulation campaigns, still operate in legal gray zones. The [Code of Practice on Disinformation](#), once hailed as a successful model of industry self-regulation, has lost momentum following the [defection of platforms](#) like X. Critically, the EU still lacks a harmonized legal definition of foreign interference, and prosecutions vary significantly. In Belgium, for example, espionage and political interference are not codified as distinct crimes, forcing prosecutors to rely on outdated corruption laws.

Institutional fragmentation hinders operational capabilities. Responsibility for defending democracy is scattered across DG JUST, DG CNECT, the EEAS, EEAS StratCom divisions, various ad hoc task forces, and others, without a centralized process to drive a cross-cutting strategy. The EU's Single Intelligence Analysis Capacity and the Rapid Alert System remain underutilized. Even in high-profile cases involving EU institutions, such as the 2024's '[Voice of Europe](#)' amplification of pro-Russian narratives or [Huawei's lobbying campaigns](#), the EU's response has been muted and timid.

Civil society organizations (CSOs) and independent media are critical first responders in Europe's democratic defense, yet they remain structurally under-supported. While funding from frameworks like CERV and Horizon Europe exists, it is often short-term, project-based, and almost inaccessible to smaller actors, most notably new entrants from civil society. Mechanisms such as the [Media Freedom Rapid Response](#) and the anti-Strategic Lawsuit Against Public Participation (otherwise known as SLAPP) [directive](#) are positive steps but remain limited in scope. Many watchdogs and investigative journalists face surveillance, harassment, and legal intimidation, with few avenues for timely protection. Although often acknowledged rhetorically, these actors are rarely treated as strategic partners. That must change. CSOs and independent media play vital, irreplaceable roles in Europe's democratic architecture. The Shield should institutionalize the role of civil society and independent media as strategic partners, not auxiliary actors.

A final critical gap lies in the relative insufficiency of current frameworks to address the evolving tactics, techniques, and procedures exploited by malicious actors. One increasingly important, yet understudied, dimension is the monetization of information manipulation. The financial incentives behind the amplification of divisive content and coordinated inauthentic behavior are frequently neglected in regulatory responses. Both foreign and domestic actors routinely exploit opaque algorithms and insufficiently regulated platform advertising policies to turn disruption into profit. Addressing these economic drivers must become a central pillar of any future-proof strategy for defending democracy.

The EUDS cannot resolve every vulnerability. But it presents a crucial opportunity to connect the dots. It must serve as a strategic framework that brings coherence to the EU's currently fragmented democratic infrastructure. To succeed, it must serve as the conductor of a broader, values-based defense strategy, one that begins at home and extends outward, protecting the democratic integrity of the Union and its allies alike. The credibility, resilience, and future of European democracy depend on whether the EU can rise to meet this challenge with the seriousness it demands.

Part 3 – A Shield for Whom and How? Translating a Concept into Action

The EU has developed a wide array of tools to defend democracy. Yet as threats become more complex, the limitations of this fragmented architecture are increasingly exposed. Internally, outdated laws, uneven enforcement, and institutional silos leave European democracies vulnerable to interference. In its neighborhood, inconsistent engagement and limited capacity constrain the EU's ability to support democratic partners under pressure. Globally, despite its regulatory leadership, the EU at times struggles to project democratic credibility in a rapidly shifting geopolitical landscape.

This is not a time for hesitation. Europe cannot afford half-measures in the face of systemic threats to its democratic foundations. As such, the EUDS must be ambitious.

In this context, the Shield presents a critical opportunity to reverse these trends and build a lasting architecture of democratic defense. To do so, it must be positioned as a flagship, whole-of-Union effort, on par with initiatives like the European Green Deal, and treated not as a siloed response but as a central pillar of the EU's entire long-term agenda. The window to act is narrowing, but there is still an opening. Now is the time to act, while the institutional frameworks and political will to support such an initiative remain strong.

The Shield must become the vehicle through which the EU demonstrates bold, coordinated, and measurable leadership on global democratic resilience. To be truly effective, it must unify protection and engagement, connect institutional responses with political will, and bridge short-term crisis management with long-term democratic renewal. It must be anticipatory, not reactive, ready to confront an evolving interference landscape with clarity and resolve.

What follows are **ten concrete recommendations to ensure the Shield is equipped to meet today's challenges, and those yet to come**. These proposals focus on the most urgent gap: foreign interference. They cover political leadership, threat recognition, coordination, enforcement, governance, and funding. While other structural challenges, such as societal cohesion and civic education, remain vital, they fall beyond the specific scope of this report.

Together, these recommendations are designed to make the EUDS worthy of its name: European in values and vision; democratic in process and outcome; and a true shield: strategic, enforceable, and built to endure.

1. See the Forest

The Shield must protect the EU from a well-thought-out barrage, not just from a few haphazard arrows. Europe is under sustained attack from a sophisticated, state-driven hybrid-warfare strategy that blends cyberattacks, FIMI operations, economic coercion, and corruption to destabilize democracies and erode their sovereignty. This is not disruption for its own sake, it is exhaustion by design. The goal is to spread chaos, erode trust, and trap democracies

in a constant state of crisis response. Europe must stop underestimating these threats and start naming them for what they are: systemic, state-driven assaults on democratic sovereignty.

The EU must see the forest for the trees and the Shield should provide a systemic response. To defend itself effectively, Europe must rid itself of factors that still hamper its ability to respond to an increasingly complex threat landscape. To address this, the EU must:

- **Adopt a consistent approach in assessing both foreign and domestic threats.** While their motives and affiliations may differ, actors on both fronts have repeatedly demonstrated a willingness to exploit similar tools to destabilize democratic processes. Currently, the EU has developed a strong repertoire of tools to FIMI, but it addresses internal democratic backsliding in an entirely different manner. This disconnect risks undermining a coherent and comprehensive defense of democratic integrity.
- **Reject the siloed thinking that treats cyberattacks, FIMI, kinetic disruption, and hybrid operations as separate problems.** A more holistic approach to threat recognition is essential because adversaries do not operate in compartments; they adaptively combine tools to exploit Europe's blind spots. This also requires more coordinated responses. For instance, while the EU has developed distinct toolboxes for cyber diplomacy, hybrid threats, and FIMI, these instruments remain largely uncoordinated. Without strategic alignment, the Union remains exposed to complex, cross-domain threats that defy traditional categorization.
- **Recalibrate key divisions between online and offline domains.** Manipulation in the digital sphere is designed to provoke real-world consequences, from polarizing elections to inciting violence, and must be addressed as part of a seamless continuum. Likewise, real-world disruptions are often mirrored and magnified in the digital realm, turning local crises into viral narratives that further disrupt and divide.

To counter this, the EU must forge an integrated approach to threat recognition, one that meets the challenge on its own terms and reflects the complexity of the threat landscape.

2. Standardize Language to Strengthen Strategy

Even the strongest shield fails if its bearer does not know what it is defending against. Without clear markings, symbols, warnings, or classifications, those holding the line are left guessing where the next strike might land. In the same way, the EUDS risks being weakened by a lack of terminological consistency.

Indeed, as mentioned in Part 2, a major challenge lies in the EU's inconsistent terminology for describing today's threat landscape, particularly across insufficiently delineated concepts like FIMI, disinformation, hybrid threats, or

cyber. Terminological vagueness muddles operational clarity, and undermines the coherence of the EU's strategic response.

To fix the problems mentioned in Part 1, the Democracy Shield must **embed a standardized and coherent vocabulary** that accurately reflects the full spectrum of interference. To advance this effort, the EU must:

- **Ensure consistency in definitions** across EU institutions and member states.
- **Expand the vocabulary to capture domestic dynamics.**
- **Clarify overlaps and distinctions** between FIMI, disinformation, cyber, hybrid threats, and other forms of interference.
- **Promote coherence in the use of the terms “interference” and “influence”** while maintaining consistency across internal and external actions.
- **Develop a unified framework** that enables clearer communication, stronger coordination, and a more cohesive strategy.

This is not just bureaucratic refinement, it is a foundational component of the Shield itself. Without shared language, there can be no shared strategy. With it, Europe can recognize, track, and defend against all forms of democratic subversion with precision and unity.

3. Enhance Situational Awareness

Every strong shield needs eyes on the battlefield. For Europe, this means continuous monitoring, early-warning systems, and shared intelligence capable of detecting influence operations and malign campaigns before they gain traction.

Today, as threats to democracy proliferate, Europe's monitoring and anticipation systems remain fragmented and reactive, marked by uneven deployment, inconsistent use of existing structures, and a backward-looking focus that limits the EU's ability to anticipate and prepare for emerging forms of malign interference.

Winning any battle requires both real-time awareness of what is unfolding and strategic foresight into what could follow. Without that dual capacity, even the best defenses fall short. With it, the Shield can move from being reactive to shaping the conditions that prevent further attacks.

To build true situational awareness, the EU should take five key steps to establish a stronger, more responsive **“Democracy Radar”** of bad actors and actions in this domain:

- **Continue developing a common framework and methodology** for identifying, categorizing, and contextualizing threats and threat actors, building on existing efforts and the solid groundwork laid by the EEAS in the FIMI domain. As it stands, the way EU institutions, member states, CSOs, and other actors register and interpret threats remains fragmented and inconsistent, undermining collective understanding.
- **Strengthen the EU's Single Intelligence Analysis Capacity and bolster efforts to establish a permanent, well-funded alert-and-monitoring process** for interference campaigns across EU jurisdictions and geographies. This process should connect existing EU structures with national authorities, civil society, and independent media, ensuring that early detection leads to a coordinated response.
- **Invest in cutting-edge digital forensics and open-source intelligence (OSINT) capabilities**, making them available to trusted partners across the defender community.
- **Embed foresight functions** into threat monitoring to anticipate and flag emerging risks, shifting from reactive to proactive threat management.
- Further down the line, **establish a regular EU-wide interference threat report** modeled on the EEAS FIMI reports to demonstrate high-level political convergence and sustained commitment to countering malign interference. This report should offer a comprehensive overview of evolving threats, track institutional responses, and identify gaps or areas for improvement. In parallel, **member states should publish annual national interference reports**, modeled on the Rule of Law cycle, to promote accountability, encourage knowledge-sharing, and reflect the unique threat landscapes and resilience capacities of each country. Together, these mechanisms would enhance strategic coherence at the EU level and operational effectiveness across the member states.

These steps can transform scattered insights into a coherent, real-time threat picture, strengthening not only Europe's defenses but also its deterrent power. When adversaries know that Europe is watching, well-equipped, and ready to respond, they are more likely to think twice before launching an attack.

4. Maximize Enforcement of Existing Tools

A shield is most effective when every part of it actively does its job and is not just polished for display. Building on the previous recommendation, the EUDS must do more than add new layers; it needs to fully activate the tools already forged. That starts with ensuring existing instruments are not just in place but are contributing meaningfully to Europe's defenses.

Among these, the DSA stands out. It offers a robust legal framework to counter online harms, including information manipulation and digital interference. Yet much of its potential remains dormant, under-implemented, unevenly enforced, and insufficiently integrated into Europe's broader democratic architecture.

To unlock its full strength, the EU must urgently shift from legislation to execution. To achieve this, the EU must:

- **Accelerate uniform implementation** across member states, ensuring no jurisdiction becomes a weak link in the digital defense chain.
- **Mandate fast, coordinated removal** of harmful content, especially during electoral periods or security crises, with clear timelines and escalation procedures.
- **Enhance platform transparency** by enforcing **standardized, timely data-sharing obligations**, particularly for researchers, civil society, and regulators involved in threat monitoring.
- **Integrate DSA enforcement into FIMI response planning**, ensuring that digital interference is **treated as an existential threat to democracy issue**, not merely a platform-management problem.

Enforcement is critical. Without strict accountability and sustained follow-through, even the strongest legislation remains just ink on paper. Activating the DSA's full capabilities will not only boost European democracies' resilience today, but will also provide the legal and operational spine for the EU's future digital defense posture. A shield, after all, is strengthened not only by adding more metal, but also by forging what is already there into a single, unbreakable surface.

5. Preserve Information Integrity

A strong Shield must prioritize the protection of information integrity, a prime target of authoritarian actors that seek to destabilize European democracies. Informed civic participation depends on access to accurate, reliable, and impartial information. This explains why anti-democratic forces, both foreign and domestic, are relentlessly attacking the information space, fully aware of its central role in sustaining democratic systems.

To preserve public trust, foster civic engagement, and support healthy democratic discourse, especially during elections, the following priority areas must be addressed:

- **Tackle the monetization of information manipulation.** Financial incentives behind information manipulation and inauthentic behavior coordination are often overlooked in efforts to counter digital interference. Malicious actors, foreign and domestic, routinely exploit ad networks, monetization algorithms, and opaque platform policies to profit from manipulation. The EU must confront this economic engine directly. This includes auditing the advertising and revenue-sharing models

of major platforms, enforcing transparency in political and issue-based online payments, and introducing regulations that eliminate financial rewards for harmful or deceptive content. Disrupting these profit motives is not just a matter of fairness but is critical to dismantling the business model of bad actors.

- **Introduce fairness in online political advertising.** Just as many member states guarantee equal opportunities in television advertising during election periods, the same principles must be extended to the online space. Digital platforms have become central arenas for political communication, but lack of regulation allows determined actors to flood the information environment with targeted, opaque, and often misleading messaging and content. The EU should support the development of national frameworks that ensure transparency, fairness, and equal access in online political advertising, particularly during campaign periods. This could include mandatory labeling that clearly identifies the sponsor of each political or issue-based ad, the amount spent, and whether the content has been targeted using personal data. It could also include spending caps to limit the total amount that political actors or third parties can allocate to digital political advertising during elections, reducing the potential disproportionate impact of high-spending entities. Finally, balanced ad-distribution requirements should ensure that platforms provide equitable advertising access to all qualified candidates and disclose how, and to whom, ads are served. Leveling the digital playing field is essential to protecting electoral integrity and rebuilding voter trust.
- **Train election officials to withstand disruptive technologies.** From deepfakes and AI-generated disinformation to automated bots that target voter rolls and amplify polarizing narratives on social media, election infrastructure faces unprecedented threats. Yet many election officials remain underprepared for this new wave of digital disruption. The EU should fund and coordinate specialized training for election administrators, focusing on the identification and mitigation of technology-driven threats. This includes scenario planning, rapid incident response, and strategic communication training, empowering election bodies with the skills, tools, and protocols needed to respond quickly and effectively.

To preserve the integrity of Europe's democracies, the EUDS must treat the information space as critical infrastructure. Safeguarding it requires not just stronger content moderation, but deeper reforms that address the financial, regulatory, and institutional conditions that allow manipulation to thrive. Without this foundation, no shield can hold.

6. Reinforce National Democratic Foundations

A shield is only as effective as the strength of each part it protects. To build a truly resilient European democracy, member states must be both supported and held accountable for strengthening their democratic governance in line with common EU standards. The EUDS should not be limited to Brussels-level action but must serve as a catalyst for reform within each country. In the short term, governments must urgently **implement the European Commission's recommendations on inclusive and secure electoral systems**. These include limiting or prohibiting third-country donations to political parties, political foundations, candidates, campaign organizations and relevant political movements, complemented by robust transparency requirements. It also requires closing loopholes such as anonymous contributions and enforcing robust rules on party financing, political advertising, and campaign spending. These safeguards remain absent or insufficient in several member states, leaving dangerous vulnerabilities open to exploitation.

In the longer term, countries must reinforce the democratic institutions that underpin open societies: independent election authorities, impartial judiciaries, empowered parliaments, and credible anti-corruption bodies. Upholding the rule of law and protecting civic space must remain central to this effort, ensuring that democratic norms are not only defended but firmly rooted across the Union.

To support this, the EU should **strengthen the link between its financial and technical assistance and meaningful democratic reform**. While earlier efforts have tied funding to principles like the rule of law, transparency, and good governance, tools such as the Rule of Law Report and the Recommendation on Electoral Resilience now offer a clearer framework for member states. The EU must build on this foundation by ensuring its resources actively drive democratic progress. Governments that erode democratic standards should face real consequences, while those that strengthen them should be supported.

Looking ahead, **the establishment of a "European Democracy Semester"**, a structured, annual review modeled on the EU's economic coordination process, could provide a consistent mechanism for assessing democratic performance across the Union. This process should incorporate insights from the annual FIMI/interference reports referenced in Recommendation 5. This would institutionalize accountability, foster uniform enforcement, and reinforce the EU's credibility as a steadfast defender of democracy from within.

7. Develop National Anti-FIMI Defenses

Even the strongest shield fails if the arms holding it are weak. The success and impact of EUDS depends not only on the instruments it deploys, but on the institutional capacity of those using them.

On paper, creating a new EU-level entity to centralize Europe's response to interference may sound appealing. In practice, however, it risks becoming a long, resource-draining distraction. Building such a body would take years—

time the EU does not have—while siphoning off political focus and funding from more immediate priorities. Worse, it could invite politicization, with adversaries branding it a “Ministry of Truth” before it even begins to operate.

The priority now must be to consolidate and strengthen the counter-interference capacity that already exists across the EU, with a particular focus on building national-level resilience. While several member states have established institutional responses, such as France’s Viginum or Sweden’s Psychological Defence Agency, others have opted for interagency coordination processes rather than creating new centralized bodies. However, too many have made little to no progress on this front. What matters most is not the institutional form, but the existence of a clear, well-resourced, and accountable mechanism to counter interference. Every EU member state should be supported in developing a mechanism that fits its national context, ensuring that it can detect, analyze, and respond to interference operations in a timely and strategic manner. Whether through dedicated agencies or coordinated task forces, these mechanisms should be given:

- **Strong political backing:** These institutions or processes are likely to become lightning rods for anti-democratic forces, both foreign and domestic. Without strong political will at the national level and a determined effort to get popular buy-in, they will not be able to carry out their mission.
- **Clearly defined legal and operational mandates:** Given the all-encompassing nature of hybrid attacks on European democracies, there is a real risk that the response to the threat either lacks focus or infringes on democratic values. It is thus essential that any effort designed to combat foreign interference is targeted and proportionate. While respecting national sensitivities, such efforts should also draw from, and ideally build upon, European best practices to ensure consistency, effectiveness, and democratic legitimacy.
- **Access to modern technological and analytical tools:** From digital information manipulation to complex financial schemes and opaque societal subversion operations, European democracies’ adversaries use all the tools that technology has to offer. National institutions must be equipped with the same level of sophistication as those threat actors. This could include access to real-time threat dashboards aggregating cyber, financial, FIMI, and other relevant indicators, as well as secure interoperable information-sharing platforms facilitating timely coordination between government agencies and trusted civil society partners.

Every member state should also prioritize sustained investment in the people and systems that will drive these efforts forward. Whether implemented through dedicated agencies or interagency processes, national structures should equip civil servants, analysts, and communications professionals with the knowledge and tools to recognize and counter complex interference operations. Continuous training is essential to stay ahead of evolving tactics.

Importantly, national efforts must be matched by stronger cross-border collaboration provided for by the EU. That means building trust among member states, improving real-time intelligence exchanges, ensuring know-how flows and exchanges of best practices, and fostering joint operational responses, especially where threats cross borders or target EU institutions.

By focusing on national capacity and enhanced cooperation, the EUDS can move from concept to capability, becoming a shared, distributed defense mechanism that draws strength from the EU's diversity and unity alike.

8. Elevate the Defender Network

A shield is only as strong as the network behind it and defending European democracy is too essential a task to be left to governments alone. If the Shield is to live up to its name, it must recognize and empower all parts of the defender community: state institutions, civil society organizations, the expert and academic community, independent and pluralist media, and citizens themselves.

Some of these actors are often acknowledged rhetorically but rarely treated as strategic partners. That must change. Each plays a distinct, irreplaceable role in the architecture of democratic resilience. The Shield must be designed with their active involvement at its core, not at its periphery.

- **CSOs and the expert community** bring deep field knowledge, flexibility, and public trust, qualities that state institutions may not always possess. Supporting their role in Europe's democratic defense entails the need to:
 - o Establish long-term funding frameworks that prioritize independence over short-term project cycles;
 - o Create formal channels for their involvement in EU-level threat analysis, response planning, and policy co-design; and
 - o Protect them from harassment, intimidation, and strategic lawsuits through legal safeguards and rapid response mechanisms.
- **Independent, pluralistic, and free media** are not only watchdogs but critical infrastructure for democracy, often the first line of defense against malign interference. These actors face mounting pressure from bad actors, regulatory overreach, and financial instability. Strengthening the Shield means that the EU must:
 - o Help media's transition to sustainable funding models, which should be facilitated by the disruption of bad actors' funding model from Recommendation 5;
 - o Protect their editorial and operational independence; and
 - o Formally integrate their insights into strategic planning and response systems.

- **Citizens**, too often overlooked, are in fact the most essential link in the defender chain. A civically literate, digitally resilient, and actively engaged population can absorb shocks and resist manipulation far more effectively than any top-down intervention. But citizen involvement must go beyond tokenistic “engagement”. It requires moves to:
 - o Further invest in civic and digital education;
 - o Create inclusive dialogue and participatory mechanisms; and
 - o Foster long-term trust-building efforts.

The Shield must elevate the role of the citizen from spectator to stakeholder. Without this societal anchoring, the Shield risks becoming a technical fix to a political and cultural problem. With it, Europe gains something far more powerful: a living, breathing defense system, strong not because it is centralized, but because it is distributed, trusted, and truly democratic.

The **creation of a Central Democracy Platform** could help foster a response that includes everyone. This could serve as the digital backbone of the Shield, bringing together funding opportunities, EU-backed programs, policy updates, and threat intelligence in one accessible space. Beyond being a resource directory, the platform should foster real collaboration: enabling civil society, media, researchers, and national institutions to share practices, access training, co-develop projects, and respond quickly to emerging risks. This is not about another portal. Rather, it is about creating the infrastructure to make democracy defense faster, smarter, and more connected.

9. Invest in Core Support for Democratic Resilience

No shield can endure if its bearer is starving. Across Europe and its neighborhood, essential democratic functions are facing an existential funding crisis. Years of investment in trusted networks and technical capacity, especially in Central and Eastern Europe and the Western Balkans, now risk being squandered. The threat does not stem from defenders’ real or even perceived failure, but from shifting government priorities and a rapid reduction in longstanding international support.

This erosion creates a systemic vulnerability. Without sustainable and flexible funding, core efforts, such as information manipulation analysis, investigative journalism, digital forensics, cross-border monitoring, and early warning systems, may falter even as threats grow more complex. The architecture that protects democracy cannot be maintained on short-term grants alone.

This is not just about expanding resources, it requires strategic transformation. Funding must be prioritized for functions that are essential to democratic resilience. Three areas stand out:

1. **Information integrity:** Investing in tools and systems that ensure the accuracy, transparency, and reliability of public information is vital to sustaining trust and disrupting manipulation.
2. **Independent, pluralistic, and free media:** A diverse and resilient media ecosystem is a cornerstone of democratic accountability and informed public discourse.
3. **Digital Forensics and OSINT capacities:** These capabilities are key to detecting, attributing, and responding to increasingly sophisticated interference operations.

To meet today's challenges, EU funding must become more flexible, strategic, and future-proof. This includes the need to:

- **Streamline proposal and reporting requirements** to reduce administrative burden.
- **Shift beyond fragmented, project-based models** to support core operations through **unrestricted funding**.
- **Enable regranting** within trusted networks to expand reach and impact.
- **Establish a dedicated rapid-response mechanism** to enable swift and scalable action in the face of emerging threats.

This is not only about resilience, but also about deterrence. When adversaries see that Europe has a robust, well-funded, and agile infrastructure ready to expose and counter interference, the cost of launching attacks on democracy rises. Resilience, in this sense, is not passive. It is strategic, anticipatory, and signals that democracy is not a soft target, but a space actively defended through sustained investment and coordinated vigilance.

10. Project Protection Outward

A shield is most effective when it safeguards not only its core but also extends protection to others, adapting to shifting threats across interconnected democratic spaces. Threats to democracy do not stop at borders, and neither should the Shield. While its foundation will remain firmly rooted in Europe, its design must extend beyond the EU, recognizing that the health of European democracy is inseparable from the strength and resilience of its allies.

Frontline partners, such as Ukraine, Moldova, and the Western Balkans, often face the same threats as EU member states, but with greater intensity and fewer institutional protections. When these partners are weakened by interference, the consequences ripple across Europe: adversaries grow bolder, interference tactics evolve, and the EU loses vital allies in the defense of democratic values.

But these states are more than their vulnerabilities, they often pioneer real-time responses from which the EU can learn. The Shield must operate as a two-way bridge: projecting support outward while absorbing insights inward.

To do so, the Shield must be anchored in a layered, context-sensitive strategy, and adaptable framework that reflects the diverse needs and political realities across regions. Adopting a **tiered model**, it should clearly set out what tools and forms of support the EU can offer at each level of engagement, and under what conditions, scaling from basic safeguards to more advanced, integrated assistance as partnerships deepen.

- **Inside the EU**, where all member states have access to the same instruments, the focus should be on coordination, enforcement, and expansion, in line with previous recommendations. Existing tools must be used to their full potential, and cross-border cooperation should be deepened to close operational gaps.
- **In the EU's neighborhood**, where tools must often be adapted to political constraints and limited institutional capacity, the Shield should offer a defined package of support, including institutional know-how, technical assistance, capacity building for the defender community, and targeted funding streams. The priority here is to reinforce independent media, civil society, and democratic oversight.
- **Globally**, the EU must continue to promote democratic norms, but with realism, humility, and strategic focus. Rather than spreading itself thin, the EU should invest in a small number of flagship initiatives, develop democracy impact assessments for trade, security, and foreign-policy decisions, and deepen coordination with like-minded partners. A smart allocation of resources, guided by a clear mapping of where the EU can add the most value, will maximize impact.

A rigid model will falter. A flexible, principled approach, backed by political will, institutional clarity, and sustained support, will ensure the Shield protects not just a geography, but an idea: that democracy, wherever it grows, is worth defending.

The Shield is a unique opportunity for the EU to lead by example, establishing a credible model of democratic defense. By embedding clear standards, fostering innovation in counter-interference institutions and processes, and lowering barriers for partner democracies to access resilience tools, the EUDS can become a global reference point in demonstrating how democracy can be safeguarded by design, both now and in the future.

As democratic backsliding accelerates worldwide, the Shield could enable Europe to offer not just inspiration, but practical and adaptable models to help others navigate the complex balance between freedom of expression, political polarization, and institutional resilience. A strong, principled, and proactive Shield could become the defining emblem of democratic defense for an entire era.

About the Alliance for Securing Democracy at GMF

The Alliance for Securing Democracy (ASD) at the German Marshall Fund of the United States (GMF) is a non-partisan initiative that exposes, analyzes, and develops strategies to counter foreign information manipulation and interference in democracies. ASD leverages its data and expertise to provide sharp analysis and actionable recommendations to counter these threats to relevant public and private sector actors. With staff in Washington, DC and Brussels, ASD translates lessons learned from countries' experiences addressing foreign information manipulation and interference for key stakeholders on both sides of the Atlantic—and, increasingly, around the world. ASD also aims to be a force multiplier, partnering with likeminded organizations to strengthen resilience among democracy's most crucial asset—the citizenry.

Acknowledgement

The authors would like to express their sincere gratitude to David Salvo, Louis Savoia, and Rita Barbosa Lobo for their steadfast support and commitment throughout the development of this report. Their contributions were instrumental in shaping its insights and recommendations.

Author Bio

Vassilis Ntousas is the senior manager and fellow for Europe for ASD at GMF, where he serves as the lead in-house expert on European foreign policy and European efforts to defend and advance democracy within and beyond European borders. Prior to joining the ASD, he was the Senior International Relations Policy Advisor at the Foundation for European Progressive Studies in Brussels, where he led the foundation's global research, advocacy, and strategic convening work. In 2019–2020, he held the Stavros Niarchos Foundation Academy fellowship at Chatham House. He is the author of several policy papers and regularly comments on global affairs for international media outlets. He is also the co-editor of two books published by Routledge, *The European Union and China's Belt and Road: Impact, Engagement and Competition* (2021) and *EU Climate Diplomacy: Politics, Law and Negotiations* (2018).

Etienne Soula is a research analyst with ASD at GMF and is based in Brussels. His research focuses on how the PRC resorts to information manipulation, economic coercion, and technology exports to weaken democracies, in the EU, United States, and their allies, and to disseminate its model of techno-authoritarianism globally. Etienne maintains ASD's authoritarian interference tracker that covers more than 700 incidents of Russian and PRC political and economic interference in Europe and North America. He also monitors and reports on PRC diplomatic and state-media messaging. Etienne previously worked at the Carnegie Endowment for International Peace, the Hudson Institute, and NATO. He holds a dual master's degree in international affairs from American University and the Université Libre de Bruxelles, as well as a law degree from the University of Nottingham.

Ankara • Belgrade • Berlin • Brussels • Bucharest

Paris • Warsaw • Washington, DC

gmfus.org