EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

POLICY BRIEF

FROM SHIELD TO SWORD: EUROPE'S OFFENSIVE STRATEGY FOR THE HYBRID AGE

Will Brown, Jana Kobzova, Nicu Popescu, José Ignacio Torreblanca

March 2026

SUMMARY

- Europe faces constant asymmetric threats. These include drone incursions, infrastructure sabotage, coerced migration, vandalism, cyber-attacks, and large-scale disinformation campaigns.
- Russia and other states, including some of Europe's partners, now aim such operations at the continent, weakening its democracies at home and its influence abroad.
- To date, European responses have mainly been defensive and based around fact-checking, digital literacy and institutional resilience.
- Europe must now go on the offensive in the information, cyber, finance and kinetic domains to counter and deter its adversaries.

Europe under quiet siege

Wars are not lost simply because of military defeat or economic exhaustion. Divided, fatigued or demoralised, people grow tired and lose the will to fight for a cause or a country. Modern warfare is fought as much in minds and cyberspace as on land, at sea, in the air and in regular space. Narratives, perceptions and cohesion can decide victory.

Aside from Ukraine, European countries are not formally at war. Yet their societies are under a barrage of attacks. Unidentified drones disrupt civilian airports. Criminal networks, often paid in cryptocurrencies, sever cables and darken railway stations in the dead of night. Neighbouring states push migrants and refugees across borders, exploiting vulnerable people to inflame tensions. Leading European business figures face assassination plots. Cyber-attackers steal or damage European innovations and black out hospital servers.

Meanwhile, on every phone and every screen, a tidal wave of lies and half-truths washes over citizens, helping turn certainty into fog, outrage into numbness. Society grows weary, mistrustful and slow to answer the call to defend itself. Europe is losing on this new front. In fact, most European countries are refusing to even fight.

To be sure, since Russia's full-scale invasion of Ukraine, Europe has not been idle. Defence spending is rising and cumbersome peacetime procedures are being streamlined. New information security initiatives and organisations, like the EU's European Democracy Shield, France's Viginum and Sweden's Psychological Defence Agency are promising first steps.

Such initiatives are a must, but they are few and far between. Overall, Europe's response so far has been largely defensive and reactive. Analysts diagnose the threats well, but the remedies they propose tend to be tame and uncontroversial: more cyber-defence, fact-checking and digital literacy, and strengthening institutions. These measures are necessary, but no battle is won with a shield alone. Sooner or later, the shield will crack and the blows will land. Europe has shown remarkable resilience absorbing many attacks, but to prevail it must learn to strike back.

This brief argues that Europe should be ready to go on the offensive in the informational, cyber, financial and kinetic domains to defend its democratic societies against a growing number of hostile actors and authoritarian states, especially Russia. The continent should push its adversaries onto the defensive by exploiting cracks in their own societies, elite networks and financial systems to make would-be attackers think twice.

Many tools are available, and many capable European states could ride out front. What is lacking is courage and determination. Without this shift, Europe will remain a placid deer amid a pack of wolves.

Anatomy of the threat

Authoritarianism is on the rise around the world. According to the latest Varieties of Democracy Index, a hub measuring democracy at the University of Gothenburg in Sweden, 45 out of 179 countries monitored shifted away from democracy towards autocracy in 2024. Only 29 countries, home to a mere 6.6% of the world's population, can now be considered full democracies. Most of them are in Europe.

Democracies are vulnerable in a world where autocratic rule is the norm, and hostile regimes are seeking to exploit that weakness. Many authoritarian states—from superpowers like China to middle powers like Iran—as well as terrorist groups have or are developing hostile influence toolkits aimed at Europe. Some focus on monitoring and intimidating diaspora communities; others directly manipulate public discourse and state or corporate policy. Many of these actors also challenge European interests and presence abroad.

In a world of increasingly "à la carte" alliances, the line between friend and foe often blurs. Many influence campaigns originate from countries with which the EU or certain member states have strong ties, such as Qatar, Turkey, Azerbaijan and Rwanda. Although they all partner with Europe in some form, whether in energy, development aid or militarily, they are also known to engage in increasingly daring offensive influence operations in Europe when it suits them, such as by targeting their diaspora populations.

The Russia problem

As of now, Russia poses the gravest threat to peace and democratic governance in Europe and its neighbourhood. Russian campaigns against European democracies are multi-platform and systematic, and have been under way for at least two decades. According to the chair of the NATO military committee, Admiral Giuseppe Cavo Dragone, Russia spends some $2bn a year on cognitive warfare. Operations are coordinated across political, economic, cultural, religious and informational spheres. They seek to weaken democratic institutions; deepen social and political divisions; and amplify radical forces, whether on the left or the right—as long as they undermine the legitimacy of the EU, pro-EU governments and Europe's reputation abroad.

Media

Official state channels are an important part of Russia's hybrid war machine. The chief editor of RT (formerly "Russia Today"), Margarita Simonyan, has said Moscow treats its state media as "a weapon like any other" that is "conducting information war ... against the whole Western world" by cultivating audiences that can be mobilised "in critical moments".

And so is social media. A secret document intercepted and published by the US Department of Justice in 2024 showed that Russian operatives are instructed to monitor influencers, identify social media trends and analyse Western think-tanks. They are also tasked with generating content, including long reads, posts, memes, cartoons and video clips, as well as building an extensive digital infrastructure across multiple social media platforms. The document reveals how Russia uses the equivalent of sleeper-cell social media groups, which only emerge with pro-Russian narratives after years of nurturing a large, trusting follower base.

These two spheres—one traditional, the other online—operate in sync, feeding off each other for content, talking points and narratives.

Some of these operations have had significant reach in Europe. In 2022, EU DisinfoLab exposed Operation Doppelganger, a major Russia-based campaign that used "clones" of authentic media like the *Guardian* and *Bild* to spread fake articles, polls and other types of malicious content designed to confuse and anger Western publics, as well as disrupt support for Ukraine.

One non-official report from the Spanish Armed Forces identified 179 actors, ranging from official Russian organisations to local influencers, disseminating Kremlin propaganda in Spain's media ecosystem in the first six months after Russia's full-scale invasion of Ukraine.

Another noteworthy example was Russia's massive operation to influence the Romanian presidential election in 2024, in which proxies helped exploit societal grievances and stir anger against the government.

Vandalism and sabotage

Russia complements media techniques with real-world actions to foment fear in communities, such as through vandalism. For example, French intelligence services believe Russia could be behind both the desecration of a holocaust memorial in May 2024 and the placing of pig heads around mosques in September 2025. The Associated Press (AP) has been tracking some of these events, and according to German intelligence, there were 321 suspected cases in Germany in 2025 alone. In the hybrid logic, images and reports of these incidents are quickly disseminated through Russia's propaganda networks at home and abroad, cutting away at Europe's social fabric and thereby reinforcing the Kremlin's position at home.

Drones

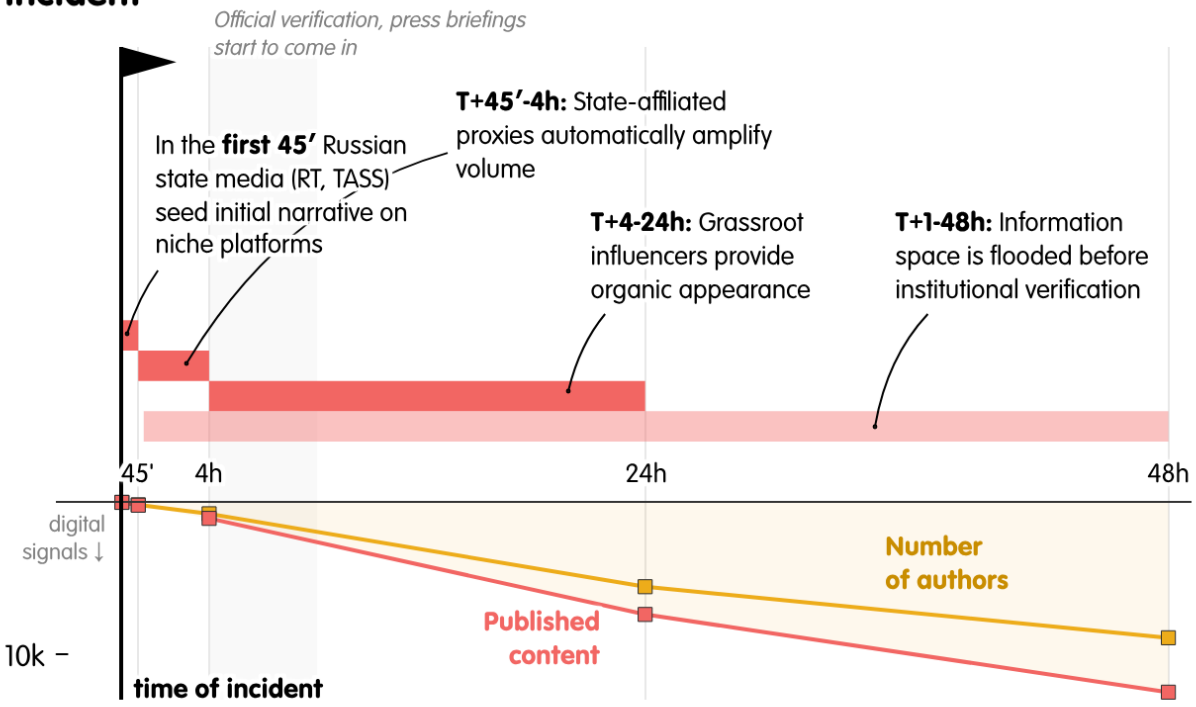
Drone incursions illustrate the logic of Russia's hybrid war well. With the help of digital media, even minor physical disruptions from an everyday drone bought on Amazon can have big impacts. Disrupting airport traffic achieves several goals at once: besides interrupting regular economic activity, it can show that authorities are unable to defend their populations, increasing anxiety or heightening dissatisfaction with governments. Incursions could also be used to frame solidarity and financial aid to Ukraine as a source of domestic instability. And governments could be forced to divert resources towards domestic defence rather than supporting allies. All of this can be achieved with a handful of drones bought for a few thousand euros in any civilian tech store.

The scale of coordination is striking. In a January 2026 study, threat consultancy Alto Intelligence documented how small, deniable physical actions are rapidly followed by coordinated online activity designed to confuse the public, assign blame and undermine trust in authorities and the wider system.

The study analysed how hostile narratives spread online following three drone-related security incidents in Europe in September and October 2025: the entry of 19-21 Russian-launched drones into Polish airspace, which triggered NATO Article 4 consultations and airport closures; a similar drone intrusion episode in Denmark; and repeated drone sightings over Munich Airport that forced the suspension of flights.

The study examined almost 50,000 digital signals—including images, videos, audio, news content and online interactions—collected across major platforms as well as niche media channels. Through this dataset, the researchers identified 25 narrative communities and tracked how coordinated networks rapidly deploy and amplify competing explanations, often within minutes of the incidents, shaping public perception before European officials have even begun to establish the facts or issue an initial explanation.

Coordinated online activity unravels within minutes of kinetic incident



Source: Alto Intelligence
ECFR · ecfr.eu

The result is that the first version of events to reach the public is frequently shaped not by evidence but by hostile actors exploiting speed, ambiguity and attention gaps.

Russia goes global

As the Kremlin seeks to expand its sphere of influence worldwide, it applies pressure on governments far from the EU's borders. In a speech at the Munich Security Conference (MSC) in February 2026, Martin Jäger, the president of the German Federal Intelligence Service, said that Moscow now has 60,000 intelligence officers worldwide, not including informants. [1] The goal of Russian operations is to shift countries' foreign policy favourably towards Moscow's interests, undermine European relationships with them and weaken support for Ukraine.

EU candidate countries

Besides its war in Ukraine, Russia militarily occupies parts of Georgia and Moldova—both EU candidates—and pours resources into political influence operations there to stoke anti-European sentiment.

Since coming to power in 2012, Georgian Dream—a political party founded by billionaire Bidzina Ivanishvili, who has deep ties to Russia—has steered Georgia towards a pro-Moscow political alignment. This trend has accelerated since Russia's all-out invasion of Ukraine in 2022. In 2024, Georgian Dream ran an election campaign playing on fears of a full Russian invasion if the country got too close to Europe, portraying votes for Georgia's pro-European opposition as siding with a "global party of war".

Since then, the government has frozen Georgia's EU accession process. It has also established a parliamentary commission to investigate those it claims were "responsible" for provoking the 2008 war with Russia, with Georgian Dream indicating that its findings could be used to ban opposition groups.

Moldova has also been hit by huge, coordinated campaigns year after year in the physical, financial and digital realms. In the 2024 presidential election and referendum on EU membership, Moscow went as far as distributing monthly payments to around 130,000 people who were expected to vote upon Russian instructions. Russia's aim is relatively simple: to keep Moldova as weak and politically unstable as possible, malleable to Kremlin-aligned oligarchs and outside Western institutions like the EU.

Africa

Russia's influence operations in Africa are best seen as an anthill, with a narrow visible structure concealing a vast underground system. Above ground are state media outlets, cultural and religious institutions, NGO fronts, journalist training programmes and high-profile diplomatic events that lend Moscow credibility. Beneath the surface, a decentralised network of paid influencers, compromised journalists, bot farms and local intermediaries tailor Kremlin talking points to local grievances, languages, idioms and worldviews.

The Wagner mercenary group and its successors have refined the industrial use of political influencers at minimal cost. This has helped to entrench anti-European messaging within key themes of African discourse, such as pan-Africanist, sovereigntist and anti-neo-colonial thought. Even before the full-scale invasion of Ukraine, Russia had constructed a substantial influence and information-manipulation infrastructure across large parts of Francophone Africa. Early operations such as Project Lakhta and front organisations like the Association for Free Research and International Cooperation (or, "AFRIC") deliberately targeted European interests in the region—particularly French and EU engagement in the Sahel—by amplifying pre-existing narratives of Western exploitation, military failure and neocolonial hypocrisy.

Since 2022, Russia's information operations have expanded considerably, spreading from Francophone Africa into Anglophone and Lusophone states and into major African languages

such as Swahili, Hausa and Amharic. This expansion has unfolded alongside Africa's accelerating digital transformation, marked by surging internet access, a young and politically mobilised population and chronically under-resourced local media.

With the help of many opportunistic and authoritarian local actors, Moscow has systematically exploited these conditions to crowd out local democratic narratives, erode trust in European partnerships and frame European diplomacy, security assistance, health initiatives and development aid as predatory, ineffective or morally compromised. In regions like west Africa, Russia works to inspire coups in democratic countries such as Senegal and boost authoritarian regimes more favourable to its interests in Mali and Burkina Faso, putting increasing pressure on Europe's southern flank.

Latin America and the Caribbean

In Latin America and the Caribbean, Russia has built an influence ecosystem that complements its anti-European messaging elsewhere. It began with RT launching a Spanish-language operation in 2009, followed by bureaus across the Americas and Europe, including in Madrid and Miami, which host large Latin American diasporas. Over the last decade, this ecosystem has enabled persistent, multi-platform messaging that is less about persuading audiences of Russia's virtues than about framing the US, NATO and—by extension—Europe as hypocritical and responsible for fuelling global instability.

These efforts are increasingly tailored to country-specific political fault lines, with ambassadors acting as legitimised spokespersons in national media and placing op-eds that translate Kremlin narratives into locally credible registers. Beneath that visible layer, there is a covert "localisation" model: Russia-linked influence-for-hire actors and proxy networks seed and adapt content through local media outlets and intermediaries so that propaganda appears organic rather than imported. The same playbook has been documented around protest cycles and elections, with Russia-linked networks amplifying unrest and synchronising message pushes across multiple countries.

Since February 2022, these channels have been mobilised as regional multipliers for Russia's global framing of the war against Ukraine—particularly the claim that food insecurity, inflation and energy shocks were primarily consequences of Western sanctions rather than Russia's invasion. Important political leaders in the region have endorsed pro-Russian views of the invasion. Brazil's president Luís Inácio Lula da Silva, for example, accused the US of promoting war by arming Ukraine; his Colombian counterpart Gustavo Petro suggested the establishment of a demilitarised zone that "physically separates NATO and Russia to guarantee permanent security to former Soviet nations". In 2023, former Mexican president Andrés Manuel López Obrador invited Russian troops to parade on Mexico's independence day.

However, some other leaders, such as Chilean president Gabriel Boric, have stood by Ukraine, reflecting public opinion in large swathes of Latin America—68% of Chilean, 64% of Mexican, 63% of Argentinian, 57% of Colombian and 62% of Brazilian voters blame Russia for starting the war against Ukraine. Indeed, despite the persistent propaganda pressure, survey-based indicators suggest Russia's overall image in the region has degraded in the wake of its aggression, including a documented decline in positive perceptions between 2015 and 2023. Moreover, in an example that may be useful in other regions, initiatives such as "Aguanta Ucrania" have shown how civil society can mobilise to counter these narratives

The trouble with Europe's response

Europeans have not been oblivious to the threats described above. Estonia, Latvia and Finland have had centres of excellence to combat disinformation, cyber and hybrid threats for a decade or more. A few weeks before Russia's 2022 invasion of Ukraine, Sweden set up its Psychological Defence Agency, while France created Vignum in 2021 to monitor digital space information attacks. Since 2018, when the European Commission published its first communication and code of practice on disinformation, member state governments have set up a rapid alert system (RAS) network to monitor and counter disinformation in coordination with EU institutions.

Parallel initiatives are also under way to adopt a convention on combating foreign operations. Organisations such as the European Political Community, the International Organisation of the Francophonie and the Venice Commission have all been exploring ways to counter election interference, manipulation, disinformation and other threats to democracy. The EU took its own steps by banning RT and Sputnik, another state-owned media network, from the bloc's media space following Russia's invasion of Ukraine. Both the EU and national governments have also taken various measures to sanction or prosecute Russian officials engaged in disinformation.

The European Commission's latest response is the democracy shield, formally unveiled in March 2024. This initiative seeks to strengthen the commission's enforcement of the code of practice on disinformation and to use the Digital Services Act to enable faster, cross-border action against influence operations. It also aims to strengthen electoral integrity by reinforcing cooperation between national authorities, updating guidance on the use of artificial intelligence in campaigns and addressing threats to political actors. The initiative will analyse political finance, especially anonymous donations and cryptocurrency, as vectors of foreign interference, with the aim of disrupting their misuse. Lastly, at the societal level, the initiative prioritises media and digital literacy, reinforces civic education and establishes a European Centre for Democratic Resilience.

Some critics say the democracy shield simply repackages existing initiatives in a typical Brussels-style bundle, and that it falls far short of both the rhetoric surrounding it and the scale of the threat. Others contend that the scheme rests on the outdated assumption that fact-checking is an effective response to disinformation, despite ample evidence to the contrary. Indeed, since at least 2014, when Russia falsely propagated that Ukrainians crucified children in the Donbas, the EU's main response has been to explain the facts and tell the truth. To this end, it established the East StratCom team within European External Action Service (EEAS), which is tasked with strengthening EU communication in its eastern neighbourhood and the local media space.

National intelligence agencies are nimbler and have more political headroom to try different tactics, which is useful. But they are often too domestically focused and poorly funded for international work. They also spend more time analysing how Europe is being hit than hitting back or seizing the narrative.

Old assumptions

After the fall of the Berlin Wall, the assumption was that democracy, liberal rights and respect for international law would spread naturally. Europe's defence of democracy then rested on a relatively narrow set of policies. At home, the EU focused on preventing authoritarian relapse, strengthening judicial independence and supporting courts and local governance. Abroad, the bloc and its Western partners prioritised supporting civil society, independent media and democratic movements through aid, trade access and political partnerships. Europe also relied heavily on US institutions and funding to lead the fight in the information sphere.

This model produced partial success in the 1990s and 2000s. But much of this was arguably due to favourable geopolitical and economic conditions that clearly no longer apply. Authoritarian powers are more assertive and better resourced, while Trump's Americahas become openly hostile to Europe. The latest US national security strategy openly expresses a desire to encourage political change within Europe, and the transatlantic relationship has deteriorated to a historic low.

Even as China began to rise in the 2000s, European officials and leaders could not countenance the end of the US-led world order. They certainly did not imagine that America would one day help demolish the very system it had designed and upheld after the second world war. Fundamentally, European initiatives and many officials' thinking on asymmetric warfare rest on assumptions from a past era, leading to risk-averse, uncontroversial and ineffective strategies today.

Existing initiatives and institutions are fragmented across regions and domains, such as civil society support and cyber-defence. They lack the critical mass required just to protect Europe's digital and media space, let alone counter infrastructure sabotage, drone incursions, political intimidation, assassination attempts and acts of politically motivated vandalism.

Lessons from then and now

To confront today's hybrid threats, Europe needs to look beyond its recent policy toolbox. Two experiences offer useful perspective: the strategic breadth of the cold war and the resilience of contemporary Moldova.

The former illustrates how democratic defence was once pursued as a full-spectrum project, extending well beyond institutions and into culture. The latter shows how such an approach can be updated for a digitally contested and geopolitically exposed environment.

Together, they show that safeguarding democracy has never been purely technical or reactive but has depended on coherent political strategy, societal mobilisation and narrative clarity.

Cold war tools

The West's cold war fight against communism and Soviet influence did not always align with the promotion or protection of democracy. The US and its allies backed several violent coups in the global south (Iran, Indonesia and Chile, among others) and tolerated authoritarian regimes in western Europe (Greece, Spain and Portugal) as bulwarks against Moscow.

Nonetheless, the era could offer selective lessons for today's challenges. A range of initiatives and actions helped nourish pro-democracy currents. These included economic aid to rebuild Europe after the second world war (notably the Marshall Plan) and concerted diplomacy. But the West also had an active cultural policy for the Soviet bloc, which involved smuggling banned books, translating clandestine literature, staging literary or music festivals and engaging with anti-authoritarian leftists.

Engagement with the Catholic Church played a crucial role in fomenting Christian Democratic parties in Western Europe; political cooperation with the Vatican in communist countries like Poland or Slovakia endowed pro-democracy movements with moral legitimacy and organisational capacity. Media such as Radio Free Europe/Radio Liberty and the BBC World Service pierced the iron curtain. They exposed, for instance, Soviet repression of the uprising in Hungary and reformists in Czechoslovakia, as well as the subsequent invasion of Afghanistan. These exposés were part of a sustained effort to ideologically attack, question and delegitimise

the Soviet regime, helping delineate and consolidate Eurocommunist movements as part of the pro-democracy, anti-authoritarian camp.

During the cold war, the US and western Europe treated such defence as a full-spectrum activity, combining hard and soft power, offensive and defensive measures, and coordination across governments, civil society and international organisations. The ideological war was not won by just correcting Soviet lies about Western democracies, but by constantly and systematically exposing the faults of communist dictatorships.

Moldovan tactics

Moldova's recent experiences in countering hybrid warfare could also offer a model for today. In 2024 and 2025, the country held several high-stakes votes—a presidential election, a constitutional referendum on EU accession, and a parliamentary election—emerging as one of the few examples of a pro-European integration government strengthening its mandate amid major instability and external interference. By combining traditional outreach, digital communication and international partnerships, Moldovans managed to integrate political, institutional and civic strategies to defend democratic institutions.

At the heart of the Moldovan strategy was proactive, big-picture politics. Moldovan leaders built a unifying meta-narrative around peace, prosperity and EU accession that addressed existential concerns like war, demography and national identity—themes that Russia typically exploits. Rather than ceding ground on conservative or traditional values, pro-EU forces reclaimed these narratives.[2]

The campaign stressed an offensive communication strategy, through which it set the agenda rather than only reacted to disinformation. Defending democracy required occupying ideological ground; fact-checking alone was insufficient. For example, when Russian proxies argued that voting for Europe meant choosing war, Moldovan officials flipped the narrative, arguing that only a pro-European government could prevent Moscow from dragging Moldova into supporting Russia's military aggression against Ukraine. This approach, rooted in credible intelligence, concrete risk assessments and public exposure of various scenarios, positioned the pro-European camp as guarantors of peace and national security. [3]

Equally crucial was coalition-building. Pro-European politics was reframed as a broad, inclusive project—a "big tent" with messages tailored to liberals, traditionalists, conservatives, Christians, trade unionists and other groups.[4]

Institutional resilience complemented the political narrative. Election-related law enforcement was visible and strict: police campaigns such as *"*don't play with your vote*"* encouraged citizens

to report corruption, while those involved in illicit finance, vote-buying or crypto-based payment schemes were detained. Authorities cooperated with international partners—including the EU, member states, the UK and many others—to track financial flows, including through blockchain forensics, and to freeze millions in digital assets tied to Russian operatives. Moldova's cyber-defence was strengthened through pre-emptive audits, equipment upgrades and a dedicated election-day cyber war room. [5] Western partners, including the EU, UK, US and Canada imposed sanctions on Russian-linked propagandists and facilitators, further increasing the cost of interference.

Civil society and independent media amplified the democratic message. NGOs, cultural figures and influencers coordinated outreach both offline and online. Door-to-door campaigns, local events and creative social-media content fostered trust and local resonance. It is hard for civic actors to beat TikTok algorithms, but pro-democracy content combined with offline campaigning proved useful in combating disinformation online. [6]

Moldova treated the defence of democracy as a continuous process, beyond immediate electioneering. Victory thus demands offensive communication, moral consistency, legal rigour and coalition-building across ideological lines. Defence against large-scale interference must occur simultaneously online and offline, informed by continuous learning from other partners.

How to fight back today

Europeans cannot copy and paste the methods of the cold war. Moldova is a country of 3 million people, and importing its lessons to a country of 84 million like Germany certainly has its limits. But there are several broad lessons from both cases that Europeans would do well to study. Chief among these is their need to move beyond a purely defensive mindset and incorporate an offensive dimension into Europe's response.

Speaking at the MSC in February, Jäger hinted at this shift. He suggested that "active countermeasures" may be necessary to counter hybrid warfare, adding that in his opinion the German intelligence service must adopt a more "operational" posture. [7]

Such cautiously worded remarks nonetheless reflect a broader inflexion point in European security thinking. Officials are increasingly willing to acknowledge that purely defensive approaches have failed to curb hostile hybrid activity, implying that attack as a form of defence is moving from the margins of strategic debate into mainstream policy consideration.

What follows is an outline for a three-pillar strategy. First, Europe needs to **defend** itself against hostile states' easy leverage or influence in European countries. Second, it needs to **disrupt** existing actions with tough defence measures. And third, it needs to **counterattack**, be more proactive and take the fight to those who undermine its democratic systems.

Defend

Pitch a bigger tent at home

Europeans need to rebuild a broader coalition for democracy at home. This will require deeper, more frequent engagement with constituencies that have often been left out of EU outreach, such as churches and other faith-based groups, as well as large diaspora communities, European or not, across the EU. One way to reach these actors in a culturally resonant way is through niche digital influencers.

Europeans should also encourage foundations to invest more in promoting democracy and social cohesion within Europe itself. There are over 180,000 foundations across 26 European countries (including Britain, Norway, Switzerland, Turkey and Ukraine), collectively distributing more than €54.5bn each year to a wide range of causes—from vaccines and green transition projects to democracy support worldwide. Yet Europe itself is fragile, and could also benefit from some these projects.

The European Commission and member states should therefore convene groups of aligned foundations and encourage them to direct more funding towards community cohesion, fact-checking and digital literacy. In many of these areas, public authorities lack the resources or flexibility to act quickly, while foundations often already have trusted access to local communities and civic networks. Mobilising philanthropic actors in this way would free up public authorities to focus on other priorities.

Improve European coordination and data-sharing

The EU's institutional response to asymmetric threats is deeply fragmented. Different parts of the Brussels ecosystem—such as the Directorate-General for Communication (DG COM), the Directorate-General for Justice, the Directorate-General for Enlargement and the Eastern Neighbourhood, and the EEAS's East StratCom task force—operate under distinct mandates and legal constraints, not to mention political cultures. The result is a patchwork of defensive activity that is no match for hybrid attacks from external adversaries.

Hostile actors frequently exploit these seams. DG COM, for example, is largely confined to communicating within EU territory, while activities the EEAS and member states fund often have no mandate to engage diaspora communities within the EU—even though these communities are frequent targets of foreign influence operations. The EU is therefore structurally constrained from operating across the very information spaces where attacks are most intense.

The EU and its institutions need far tighter coordination and a shift in assumptions. For the purposes of democratic defence, countries seeking accession should be treated as if they were already member states. Indeed, as seen in Ukraine before 2022, in Moldova and in Georgia, EU candidates are often the main targets of the Kremlin's information warfare. The EU should include them in its communication campaigns, in formal engagement with digital social media platforms, and in the use of EU tools to expose and counter hostile information operations. That requires alignment not only of strategy, but of budgets, mandates and legal authorities across institutions.

As a practical step, the EU should establish a network of "democracy shield sherpas" across member states, backed by a major boost for the RAS's purview and resources. Their task would be to coordinate national and European responses to asymmetric threats, ensuring political ownership at the highest level to drive rapid, cross-border action when European democracies come under attack.

Finally, the EU and member states must create mechanisms to automatically share data on asymmetric attacks, whether they are digital or physical. Too often information on such attacks is relayed by ad hoc diplomatic channels or back channels when Europeans need real-time reporting and alert systems in order to stop them.

Boost funding for trustworthy local and international outlets

One of the simplest, and least controversial, things European governments must do is to boost funding for respected media outlets like the BBC World Service, Germany's public broadcaster Deutsche Welle, and Radio Free Europe/Radio Liberty. These organisations still have immense reach and credibility across much of the developing world. It is an act of wanton self-destruction for governments and officials to cut funding to rigorous, independent media outlets with international reach at just the moment when Europe's adversaries are pouring billions into their propaganda machines each year.

The EU and national governments should award grants to local media outlets across Europe, which often command the most trust locally but are collapsing under the weight of social media algorithms and generative AI. Parallel support should help cash-strapped non-European newsrooms access reliable wire services such as AP, Reuters and the French state news agency, Agence France-Presse. This would counter the flood of propaganda pouring into large parts of the developing world from state-controlled media houses such as RT, Sputnik and China's Xinhua News Agency.

The EU and member states will also have to develop innovative ways to engage online communities, through influencers, stand-up comedians or religious leaders active on social media.

Disrupt

Counter incoming drones as a pan-European effort

Drones are likely to remain an easy, cheap way for Europe's opponents to disrupt air traffic, damage institutions and, as a result, influence public opinion. Europeans urgently need a new approach to drones, both in terms of legislation and, even more importantly, capacity to detect, identify and intercept incoming drones.

Currently, no country in Europe has better skills and greater capacity to do that than Ukraine, and many EU and NATO states are increasingly collaborating with Kyiv in this sector. However, this is mostly done on a bilateral basis. Using the "coalition of the willing" format, Europeans should enhance drone cooperation with Ukraine to allow greater mutual learning, scaling up of counter-drone systems, joint drone development and production, and shared protocols for drone detection and interception.

Tackle financial crime

The EU and member states urgently need to take action to halt and disrupt flows that fund attacks on democracy. Those engaged in online disinformation campaigns and offline subversive actions increasingly rely on cryptocurrencies, though cash payments and payments through regular bank accounts remain common. In Ukraine, Russia has used cryptocurrency to lure young people, including minors, into subversive actions to undermine mobilisation efforts and security. Russia has used similar techniques in Moldova and in acts of sabotage across the EU. Some national cyber police units are already taking action, but the EU should expand the use of its banking regulators, criminal investigators and sanctions authorities to trace and examine illicit sources of financing, including cryptocurrency.

Disinformation thrives because it pays. Operatives often function as entrepreneurs, selling their technical capacity, influencer networks, bot farms and content-production services to the highest bidder in an information marketplace. A single coordinator can run hundreds of accounts or micro-influencers, making substantial sums from their operations. Europe should aim to progressively introduce grit into the system through measures such as tax probes and state-sanctioned cyber operations against crypto wallets and other infrastructure used to fund disruptive actions. Europe needs to increase the cost of this business model, including by prosecuting and investigating bosses and influencers who live in luxury in Western countries. To this end, member states should give intelligence and security agencies full authority and legislative headroom.

Use the judiciary

It is rare for propagandists working for adversary states on European soil to be prosecuted. European laws often favour authoritarian or kleptocratic actors in silencing investigative journalists and commentators—through libel suits or strategic litigation, for example. Criminals working on behalf of a foreign state to sabotage critical sites are more likely to be prosecuted for vandalism than espionage. On top of that, European judicial systems move at peacetime speeds.

European citizens and residents who take money or operate on behalf of foreign adversaries should face far tougher legal penalties. Legislation across member states should recognise that even low-intensity, seemingly disconnected acts of sabotage and subversion can carry strategic implications for national security.

EU member states must disrupt the disruptors of democracy. They should establish cross-national task forces for rapid response through sanctions, joint investigative teams into malign influence networks and coordinated hostile actions against the EU.

The challenge is both structural and practical. There is no EU-wide level legal definition of sabotage or an agreed framework for potential responses, as these issues fall into the purview of individual member states. Without overstepping its mandate, the EU could convene a platform or task force for member states to voluntarily coordinate national legislative responses and share best practices.

Shut down and defund the platforms

Many European elections in the last decade have witnessed Russian attempts to influence outcomes by amplifying anti-EU narratives and supporting far-left or far-right pro-Moscow forces. During the covid-19 pandemic, Russia also consistently propped up anti-vaccine movements, safe in the knowledge that anything which discredited political institutions and sowed polarisation played to its advantage. The EU did not do much about this until the (second) Russian invasion of Ukraine in 2022, when the bloc banned RT and Sputnik from its media space.

But this did not stop Russia using social media to undermine election integrity, as seen for example in Romania's December 2024 presidential election. Platforms such as Telegram are well known conduits of Russian or extremist propaganda networks, and its algorithms and paid promotion tools often steer users towards channels linked to these groups.

Meanwhile, Elon Musk, the owner of X, has visibly and publicly aligned with Russia by turning his website into a platform of support for the far-right Alternative for Germany party in the country's general election in February 2024 and the far-right Southport rioters in the UK in October that year.

Social media is a powerful tool for connection, expression and civic participation. But the biggest social media companies of today are de facto monopolies concentrated in the hands of a single political or ideological operator—in the case of X, one that actively promotes far-right policies and narratives across Europe.

The continent clearly needs a more open, plural and competitive social media market. Solutions exist: through interoperability and portability, which allows platforms to share core functions, smaller companies and start-ups can plug in into dominant ones, reducing user lock-in and giving citizens real choice without losing their networks or data.

While these solutions build a greater presence, Europeans have other powerful tools to counter foreign interference through social media. These include the Digital Services Act, which allows for the punishment of platforms that let disinformation and fraud spread unchecked. The EU could also use the Digital Markets Act to prevent platforms from abusing their market power. Europeans should also consider national-security tools similar to the American legislation used against TikTok, the "Protecting Americans from Foreign Adversary Controlled Applications Act", which bans apps controlled by entities from designated foreign adversaries, such as China, Russia, Iran and North Korea. An EU equivalent could mirror this via the Digital Services Act's Article 39 (systemic risk mitigation) or the Anti-Coercion Instrument. App stores could enforce portability during phase-outs.

Europe cannot ignore social media services that are clearly threatening its democratic processes through disinformation, which is a lucrative business. The EU and member states must therefore smash the link between money, advertising, attention economies and disinformation with every tool at their disposal.

Counterattack

Europeans must learn from the offensive methods employed by Russia and other authoritarian powers. This does not mean embracing post-truth rhetoric or the dishonest practices that corrode democratic, rules-based societies. Nor does it mean merely trying to "modernise" official EU or national communications to better suit social media.

It means building the know-how, the institutions and the digital infrastructure to conduct offensive information operations when Europe is attacked. This includes offensive ideological

strikes that question and delegitimise dictatorship and authoritarianism in the offending countries themselves. If done properly, these actions have a deterrent effect.

Some schemes already exist but, understandably, they are not public. Here, Europeans can learn a great deal from Ukrainians, who have developed excellent cyber-defence and strategic communications abilities and psychological warfare tactics to demoralise enemy soldiers. For example, Ukraine's "I Want to Live" operation is one publicly reported case study, which is believed to have been highly successful in convincing many Russian soldiers to surrender.

European agencies hold vast amounts of material that could distress and disrupt their adversaries. What is missing is the funding, the procedures and a hard-nosed culture to ensure this information reaches audiences in forms they trust and understand. Europe should not shy away from using local proxies, influencers and informal networks—online and offline—to disseminate narratives that undermine hostile regimes. European actors working in this space must be able to move fast, operate at scale and tailor their messaging to local contexts, languages and cultures.

EU institutions are not designed for this type of activity. Many of their efforts should therefore be conducted at arm's length. Europe already has deep reservoirs of relevant expertise: former journalists, communications professionals, digital marketers and grey-zone operators who are often better equipped for this terrain than diplomats or bureaucrats.

Carefully calibrated commercial and institutional incentives could foster a more dynamic ecosystem without concentrating dependence on a few large contractors. Britain, Ukraine and the Baltic states, which have developed some of the most advanced practices in countering hybrid warfare, should play central roles in these efforts.

At the same time, European states need to be ready to use asymmetric attacks in the kinetic and cyber spheres that undermine their adversaries' capacity to do them or their allies harm. This is a grim but necessary chapter. Ambivalence is understandable in peacetime; not any more.

Regulatory and operational frameworks built for a slower, more benign world must adapt to the fast tempo of today's conflicts. For now, Europeans have mainly relied on the waning resilience of their democratic systems rather than proactive measures. But unless the adversaries start feeling the costs of their actions, they are unlikely to stop.

Several EU and NATO countries are deploying cyber tools and taking increasingly proactive steps. Even those without such capabilities could do more now: wage more proactive communication operations in their opponents' societies, undermine these regimes' pillars of support, and sanction the instruments and entities used for subversion, disinformation and sabotage against Europe.

Cold, cognitive and hybrid

A European looking out at the world in the cold light of day sees many foes and few reliable friends. Adversaries are exploiting the openness of Europe's democracies to undo democracy itself. Its citizens may live in peace now, but a full-scale war on their perceptions is already under way.

This war is cold, cognitive and hybrid. Its weapons—sabotage, coordinated disinformation, illicit finance and deniable cyber-attacks—aim less at territory than at public trust, industry and democratic will. Defensive fixes alone will not do. Europe must move from reaction to a posture that also disrupts and pushes back.

The EU and member states have launched strong initiatives, but they are nowhere near enough. They should be seen as a starting point: a good base to rapidly expand action from. Adapting to the battlefield is now crucial for survival.

The old world is gone. Mourning it will not help. Europe may not have wanted this, but Europe is now at war. If it wants to protect its peace and prosperity, it will have to fight.

About the authors

Will Brown is a senior policy fellow with the Africa programme at the European Council on Foreign Relations.

Jana Kobzova is co-director of the European Security Programme and senior policy fellow at the European Council on Foreign Relations.

Nicu Popescu is co-director of the European Security Programme and distinguished policy fellow at the European Council on Foreign Relations.

José Ignacio Torreblanca is a senior adviser and distinguished policy fellow at the European Council on Foreign Relations.

Acknowledgments

The authors would like to thank the Spanish Ministry of Foreign Affairs, European Union and Cooperation, for their support for this project, as well as Carla Hobbs, director of ECFR's Madrid Office. The policy brief owes much of its form to the crisp edits of Taisa Sganzerla and its graphs to Nastassia Zenovich. Thanks also go to Jonathan Paul Craig Nelson from Alto Intelligence for their much-valued collaboration.

[1] Martin Jäger, speech at the Munich Security Conference, Germany, February 2026.

[2] Authors' conversations with Moldovan officials, Chisinau, 2024-2025.

[3] Authors' conversations with Moldovan officials, Chisinau, 2024-2025.

[4] Authors' conversations with Moldovan officials, Chisinau, 2024-2025.

[5] Authors' conversations with Moldovan officials, Chisinau, 2024-2025.

[6] Authors' conversations with Moldovan officials, Chisinau, 2024-2025.

[7] Martin Jäger, speech at the Munich Security Conference, Germany, February 2026.

ABOUT ECFR

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy. ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU's member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Carl Bildt, Lykke Friis, and Norbert Röttgen.

- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia, Warsaw, and Washington. Our offices are platforms for research, debate, advocacy and communications.

- Developing contagious ideas that get people talking. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to carry out innovative research and policy development projects with a pan-European focus. ECFR produces original research; publishes policy reports; hosts private meetings, public debates, and "friends of ECFR" gatherings in EU capitals; and reaches out to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions. ecfr.eu

 ISBN: 978-1-918078-24-4 – ECFR 628. Published by the European Council on Foreign Relations (ECFR), 4th Floor, Tennyson House, 159-165 Great Portland Street, London W1W 5PA, United Kingdom.