CARNEGIE
EUROPE

JULY 2026

Assessing Information Ecosystems: How Governments Can Get Ahead of Hybrid Threats

Raluca Csernatoni
Alicia Wanless

Assessing Information Ecosystems: How Governments Can Get Ahead of Hybrid Threats

Raluca Csernatoni
Alicia Wanless

July 2026

About the Carnegie Endowment for International Peace

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 200 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

Carnegie Europe
Rue du Congrès, 15
1000 Brussels, Belgium
P: +32 2 735 56 50
CarnegieEurope.eu

This publication can be downloaded at no cost at CarnegieEurope.eu.

TABLE OF CONTENTS

About the Authors

Raluca Csernatoni is a fellow at Carnegie Europe, where she works on European security and defense, with a focus on emerging and disruptive technologies like AI.

Alicia Wanless is the director of the Information Environment Project at the Carnegie Endowment for International Peace, which aims to foster evidence-based policymaking for the governance of national information ecosystems.

Carnegie Europe

Carnegie Europe delivers interdisciplinary expertise and independent insights that bring together national, regional, and global perspectives and help European policymakers grasp and respond to global challenges. From Brussels, we focus on three themes: the European Union's relations with its partners and competitors; the risks of democratic backsliding in Europe and around the world; and Europe's efforts to meet today's most pressing global challenges, from climate change to the new frontiers of cyber diplomacy.

This working paper was produced in the context of the EU Cyber Direct–EU Cyber Diplomacy Initiative project with the financial assistance of the EU. The contents of the paper are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the positions of the EU or of any other institution.

Introduction

For the past twenty years, militaries and civilian policymakers alike have increasingly adopted the term "hybrid warfare."[1] Originally used to characterize a mix of conventional and unconventional tactics in warfare, the phrase now serves as a catchall for nearly any destabilizing action, spanning multiple domains from cyber attacks and drone threats to disinformation, economic coercion, and election interference.

Yet, hybrid as an organizing concept blurs important legal and operational distinctions across war, peace, coercion, competition, and endogenous democratic dysfunction. As a policy shorthand, the term remains useful. As an analytical framework, however, it often obscures more than it clarifies. The purpose of analysis is to provide evidence-based insights to inform goal setting and strategic choices in decisionmaking. Beyond confirming that adversaries use all kinetic and nonkinetic tools and methods at their disposal, and imagining the near-mythical powers they may wield as a result, the concept of hybrid threats falls short when it comes to outlining pragmatic courses of action.

Consequently, grouping various threats together can only go so far in addressing them.[2] Many of these threats are deeply interconnected, and all of them play out to some degree in the global information environment and in complex national information ecosystems. What is more, despite being categorized under a single umbrella of hybridity, many threats are addressed in separate mandates with little coordination across silos. This can be seen in the many European governments that have set up offices or sections for hybrid threats. While often tasked with producing systematic assessments of the impacts of hybrid threats and enhancing national coordination, most of these departments lack the capacities and authority required to establish such capabilities because of poor broader awareness and interdepartmental competition.

In the European Union (EU), disjointed decisionmaking in a rapidly changing, complex operational environment leaves policymakers in Brussels and national capitals without clear strategies, institutional roles, or resource plans that can collectively address such threats. The gap between the need to understand this environment holistically and the continued siloed implementation of targeted solutions is not only growing but also, in turn, increasing the complexity of security planning and governance responses. Instead of focusing solely on ever-changing threats, security stakeholders must step back and understand the system in which they occur: the dynamic ecosystem whose conditions shape how a nation experiences and addresses emerging challenges.

This means situating those threats in the context of information ecosystems to understand what conditions foster resilience against them, with the aim to better inform strategies and coordinated responses in an interconnected, dynamic operating space. This approach would shift the analysis from isolated incidents to a shared vulnerability mapping across sectors:

coordinating across cyber, infrastructure protection, platform regulation, economic security, and democratic resilience; connecting tech sovereignty to the governance of critical infrastructures; and helping policymakers prioritize intervention when cross-domain vulnerabilities are most likely to cascade into political crisis. Apart from mapping gaps, this approach would also provide meaningful indicators for upgrading the administrative, procedural, and legislative layers of governance, capacity, and capability to enhance national resilience.

An ecosystems approach addresses not only the coordination failure but also the conceptual failure by insisting on precise categorical distinctions between adversarial action, infrastructural fragility, and emergent dysfunction and by identifying the conditions, actors, and feedback loops that produce each. Whereas the hybrid concept lets analysts group heterogeneous phenomena under a single label, an ecosystems analysis forces them to specify which relationships are being disturbed in which system, by whom, on what time scale, and with what institutional consequences.

Ecosystems are constantly changing. They are shaped by regulatory choices, infrastructural investments, and institutional arrangements. Hybrid framings tend to obscure this fact by treating threats as exogenous shocks to an otherwise healthy order. These framings ignore how ecosystems evolve, how they shape decisions and are shaped in return, and how they might be made more resilient. Improving resilience means looking past individual threats to the ways polities make and unmake the conditions of democratic contestation.

For the Love of Hybrid

European policymakers have increasingly embraced the hybrid concept. In March 2026, the EU Council adopted wide-ranging conclusions on advancing the union's ability to counter hybrid threats.[3] The conclusions referred to the EU Hybrid Toolbox, the second directive on network and information systems (NIS2) and the directive on Critical Entities Resilience (CER), the Cyber Diplomacy Toolbox, the Digital Services Act, the Foreign Information Manipulation and Interference (FIMI) framework, the European Democracy Shield, and sectoral strategies that cover maritime, airspace, cyber, and critical-infrastructure resilience alongside passing references to artificial intelligence (AI) and quantum technologies.

This was an important effort to catalog existing instruments. But the task is no longer simply about "reaffirming" instruments, as in the council's conclusions, or adding new ones.[4] It is about organizing them around a clearer theory of how vulnerabilities interact in the same operating environment. The conclusions demonstrate this partial advance: maritime in one section, airspace in another, cyber in a third, and FIMI in a fourth. What is missing is a strategic vision matched by an operational logic that can make sense of and connect infrastructural disruptions, technological dependencies, information manipulation, and practices of economic coercion as disturbances in the same wider ecosystem.

At the moment, each of these evolving threats tends to be addressed in its own policy community with its own set of instruments. EU institutions have sought to build bridges across these silos through cross-cutting mandates, such as the European Democracy Shield; FIMI work; regulation of online platforms; rules on AI, cyber, and critical infrastructure; and wider initiatives on digital democracy and cyber diplomacy.[5] The problem, then, is not a lack of coordination language or will to synergize across policy domains. Rather, existing coordination is often rhetorical, procedural, operationally ineffective, and too domain specific to explain how vulnerabilities traverse the same ecosystem.

For instance, the EU's Action Plan Against Disinformation, the European Democracy Action Plan, and the more sophisticated FIMI framework have helped professionalize responses to foreign interference and platform manipulation. Yet, they still tend to treat the information environment primarily as an online space polluted by harmful content from external vectors. What gets lost are internal vulnerabilities, such as local trust networks, legacy and community media, institutional credibility, commercial incentive structures, and the digital and civic infrastructures through which people interpret and act on information. Even when the EU supports initiatives on digital democracy, media pluralism, civic tech, and digital citizenship, these efforts are peripheral to the main architecture for security (including cybersecurity), platform regulation, and FIMI. In short, they are rarely connected to a wider analysis of information ecosystems.

Meanwhile, emerging and disruptive technologies are significantly enhancing threat actors' capacities and turbocharging the risk landscape.[6] Generative AI systems can already scale the production of synthetic content dramatically, while agentic AI tools could enable more adaptive and semiautonomous malicious campaigns across informational, cyber, digital, security, and economic domains.[7] The result is a widening gap between what these systems can now do autonomously at machine speed and what European legal, administrative, security, and democratic institutions can comprehend and govern on human time scales.

These technologies are complicating a threat landscape that already defies easy categorization. This situation in Europe is now compounded by debates about the need to deregulate and reduce red tape, struggles to establish tech sovereignty, and asymmetric dependencies on foreign-controlled digital infrastructure. Russia, China, the United States, and a growing array of rogue actors, from state-linked hacker collectives to private cyber-mercenary firms, are exploiting every weakness in Europe's fragmented framework of responses to hybrid threats.

Moreover, the convergence of large language models with the Internet of Things, smart city infrastructures, digital platforms, and autonomous systems creates new threat vectors and enables a previously unseen scale of surveillance and access. Adversaries can exploit AI-generated content to manipulate the inputs of automated decisionmaking systems in critical infrastructure, producing cascading effects that bridge the informational, the digital, and the physical. For instance, an emergency alert about an AI-driven deepfake, disseminated

through compromised smart city communication systems, could trigger panic, overwhelm emergency services, and create physical damage, all without a single kinetic weapon being deployed.[8]

These different types of threat are interrelated; as such, they must be understood not only individually but also collectively—not simply as a categorical grouping, but for how they interact. That requires a flexible framework that can address individual threats with specific expertise while scaling up to understand and deal with systemic risks, moving fluidly between these scales.

For example, three distinct problems deserve attention. The first is the possibility of deliberate aggression. Think sabotage, election meddling, or a cyberattack. Someone is behind it, pursuing a goal, though identifying the perpetrator is often hard. The second problem is carelessness or greed. Infrastructure firms, platforms, and tech providers make ordinary business choices that leave the system weak. They (sometimes) mean no harm, but harm results. The third issue is drift. Actors interact within an ecosystem, and the whole behaves in ways no one person or company controls.

Lumping these problems together is a mistake. The risk in doing so is that everyday commerce is treated as a security threat or that hostile acts are seen as mere market failure. The first challenge calls for sanctions, counterintelligence, deterrence, or law-enforcement action. The second requires rules, regulatory oversight, and liability. The third calls for systemic monitoring, institutional adaptation, and resilience building. A good ecosystem approach keeps the three distinct while tracing how they feed into one another.

In this respect, the 2026 security landscape requires a different conceptual approach: one that moves beyond grouping individual threats together to understanding the systems in which these threats exist. It is not enough to classify threats and address them through separate corresponding countermeasures: Cyber threats require cyber defenses; disinformation requires counternarratives; tech sovereignty requires investments and the reduction of critical capability dependencies; economic coercion demands trade tools.

If Europe cannot connect threats across domains, it will not be able to address them effectively, especially amid rising social costs and shrinking budgets. Moreover, focusing on threats alone will not lead to resilience. Indeed, with the scale and scope of these threats expected to increase, figuring out how information ecosystems can be made more resilient against them is key. That starts by taking an ecosystems approach, which means changing the unit of analysis and the organization of the response: mapping dependencies, coordinating across silos, and intervening where vulnerabilities are most likely to cascade.

An Ecosystems Approach

Recent research on information ecology suggests that information ecosystems can be analyzed in much the same way as physical ones.[9] Both are complex systems of inputs, outputs, conditions, and processes in which entities interact with each other and with their respective environments. This ecological perspective reinterprets security threats as disturbances in a wider ecosystem, whose overall health or decline influences the resilience of democratic decisionmaking, including all institutional and individual decisionmaking alike.[10] Knowing how to withstand a disturbance or recover from one requires an understanding of what the information ecosystem is and how it functions.

Information ecosystems form within the wider, global information environment. These complex and adaptive systems emerge from the relationships between humans, tools, information, and the surrounding context, including structural conditions, such as the economy, governance, or security. These ecosystems have existed as long as humans have been able to communicate, yet they remain poorly understood. At their core, they consist of actors, infrastructures, information flows, institutions, incentives, and shared practices of meaning making. "Information ecosystem" is a term that is often used but seldom defined, and when it is, it can mean something slightly different with each mention. Each field sees these ecosystems through its own lens. Many people use the term to mean the internet or social media, as in the focus of EU efforts to counter disinformation, while some might mean news media, and elsewhere, it is a stand-in for an organization, like a business.

Part of the confusion lies in the fact that varying factors in information ecosystems can lead to various scales and types of them, much as a tiny tidal pond is an ecosystem in the physical world, as is a rainforest. An information ecosystem can be a specific organization or place, such as an airport, where travelers, airlines, and airport staff share information about flights. It can be national and territorially bounded, shaped by law, language, infrastructure, and geography, as in the case of Ukraine or the Baltic states under persistent informational pressure from Russia. It can also be transnational and virtual, forming among dispersed communities connected by shared identities, platforms, or professional networks. Big or small, every information ecosystem consists of people, tools, and outputs connected through interrelationships and bound by a shared idea or organizing context, such as a religion, an identity, an institution, or a nation-state.

Because they are formed through relationships, information ecosystems are dynamic and constantly changing. Populations fluctuate. Skills for processing information shift. Resources and knowledge shape what tools develop, which, in turn, changes the types of output available. Throughout these changes, ecosystems usually retain their structure—unless a closure or collapse occurs. All ecosystems develop over time and build on what came

before. Information ecosystems have existed since people learned how to communicate, beginning with gestures. People developed language (a tool) that they could speak (an output) to share ideas. And from there, every new tool (like a writing system) led to more outputs (like written messages), with each innovation adding more complexity to the ecosystem.

Today, much of everyday communication depends on the internet and the complex digital, infrastructural, and energy systems that sustain it. Things like language and writing have not disappeared; they simply remain the basis for most of the means and outputs humans use to communicate today. However, the more a society relies on digital technology to produce, share, and store most of its outputs for nearly every aspect of daily life, the more inherently fragile that information ecosystem becomes. That is increasingly apparent with every cloud outage. When Amazon Web Services goes down, so do airlines, banks, government departments, and healthcare providers.[11]

But the fragility of modern national information ecosystems is due not just to potential cloud outages. Amid major geopolitical shifts, sovereignty concerns are also emerging in countries that depend on technology made elsewhere.[12] Categorizing threats under the hybrid umbrella helps organize them when the discourse focuses on adversaries, whereas an actor-agnostic ecosystems approach helps observers to understand the vulnerabilities that arise from complexity and geopolitical shifts. Such an approach also reduces the risk of threat inflation, which attributes to foreign malign actors what are, in significant part, endogenous problems of socioeconomic governance models in democracies: commercial incentive structures that reward sensationalism, platform architectures that amplify outrage, and the long-term erosion of institutional trust through domestic political choices.

Hybrid framings obscure these factors by positing an exogenous adversary acting on a domestic body politic that is otherwise assumed to be healthy. In reality, hostile operations typically exploit vulnerabilities that are domestically produced: concentrated ownership, algorithmically amplified polarization, hollowed-out local journalism, the capture of public discourse by private engagement metrics, and the ordinary erosion of institutional trust through domestic political choices. An ecosystems approach returns responsibility to the polity that makes these conditions and can therefore unmake them.

Putting Hybrid Threats into Context

Looked at in the context of information ecosystems, the relationships between various hybrid threats become clearer. The sabotage of undersea internet, gas, and power cables in the Baltic Sea, the systematic risks posed by Russia's shadow fleet to maritime safety and critical infrastructure, disruptive drone incursions into EU airspace, and the deliberate jamming and spoofing of global navigation satellite services across Europe all exemplify hybrid threat vectors that operate at the intersection of physical infrastructure and information

ecosystems.[13] The EU Council's March 2026 conclusions on hybrid threats recognized these domains, calling, for instance, for improved maritime situational awareness and coordinated responses in airspace.[14]

However, the council's approach remains domain specific: Threats in maritime, airspace, and cyber sectors are discussed separately, with no analytical framework to understand how adversaries coordinate disruptions across these domains to create cascading effects that are simultaneously physical, digital, informational, and psychological. Taken one by one, each incident—and its response—sits in a separate dossier. The 2024 sabotage of the C-Lion1 and Estlink 2 cables under the Baltic Sea, and the subsequent detention of the shadow-fleet tanker *Eagle S* in Finnish waters, is a critical-infrastructure problem.[15] The Romanian government's declassification of intelligence and the Constitutional Court of Romania's unprecedented 2024 annulment of a presidential election—over a mix of coordinated TikTok amplification and platform manipulation, suspected Russian interference, and concerns over campaign financing—fall under the EU's FIMI framework and, possibly, its Digital Services Act.[16] Yet, both examples trace the same operational logic: adversaries probing the seams between the infrastructural, informational, cognitive, and institutional layers of a single, Europe-wide ecosystem to test where the stitching gives way first.

An ecosystems approach to security acknowledges that the vulnerability of critical infrastructure arises from weaknesses in its internal security measures and from the wider technological, informational, cognitive, and institutional environment in which it operates. A power grid whose operators are targeted by sophisticated psychological operations is vulnerable even if its firewalls are impregnable.[17]

Disputes over access to Starlink in and around Ukraine exposed, with unusual clarity, the risks of Europe's reliance on privately controlled foreign digital infrastructure and the geopolitical leverage such dependence can create. In 2022, tech billionaire Elon Musk, who had developed the satellite-based internet service, refused to activate it in Ukraine to enable an attack in Crimea, and in 2025, U.S. President Donald Trump threatened to switch off the satellites to force Kyiv to make concessions in peace talks.[18] For the EU, these disputes serve as a reminder that tech sovereignty goes far beyond creating European alternatives to U.S. or Chinese platforms. Sovereignty requires ensuring that the infrastructural foundations of European security—from satellite communications to cloud computing and AI development—are democratically governed rather than subject to the strategic calculations of foreign governments or the commercial interests of unelected tech magnates.

The European policy discourse has treated tech sovereignty largely as an industrial and economic objective, such as reducing strategic dependencies, fostering indigenous innovation ecosystems, or securing supply chains for critical components.[19] These goals are necessary, but they are only part of the picture. Viewed through an ecosystems lens, tech sovereignty is also about a polity's capacity to exercise meaningful authority over the technological infrastructures that shape its critical defense systems and democratic processes. It is, in other words, a question of who governs the digital architectures through which contemporary

power is exercised, on what terms, and according to which values.[20] This is why proposals for a European digital sovereignty stack, including the EuroStack initiative, should frame infrastructure not just as a layered catalog of material and digital components to be procured but as a set of knowledge systems and political institutions to be built, governed, and maintained through democratic deliberation.[21]

Tech companies increasingly control critical resources, data, algorithms, cloud infrastructure, and satellite networks that mirror the capacities traditionally monopolized by sovereign states.[22] An ecosystems approach recognizes that not only tech-capable states but also rogue or foreign agents—whether state-adjacent hackers, cyber-mercenary firms, or Big Tech companies that exercise geopolitical power without democratic mandates—are all dynamic parts of information ecosystems shaped by regulation, deregulation, privatization, and the blurring of civilian and military boundaries. Taking an ecosystems approach makes it possible to track how these actors change over time, which conditions enable which types of behavior, and how feedback loops might amplify their impact.

These actors occupy distinct positions in the ecosystem and should not, of course, be flattened into a single category. State-adjacent hackers and cyber-mercenary firms conduct recognizably offensive operations outside or at the edge of legal frameworks and call for responses drawn from counterintelligence, sanctions, attribution, and law enforcement. Dominant tech platforms wield geopolitical weight of a different character. Their influence derives from scale, infrastructural dependence, lobbying power, and the commercial architectures through which they mediate knowledge production, speech, commerce, and critical services. Their activities, however consequential, are generally conducted within legal frameworks and call for responses drawn from competition policy, platform regulation, human rights protections, and democratic accountability.

An ecosystems approach traces how both kinds of actor shape ecosystem conditions while analytically separating the forms of power they exercise and the institutional responses each warrants. The EU's Digital Services Act and Digital Markets Act are the most direct European attempts to discipline tech giants through ecosystem-level rules on systemic risk assessment and algorithmic transparency to create a safer and more competitive digital space and make market conduct more predictable. However, these acts' effectiveness, the strength of their enforcement, and the issue of whether further tools will be needed as agentic AI and integrated platform ecosystems evolve remain open and consequential policy questions.

Weaponized Interdependence

Interestingly, the way tech sovereignty intersects with what scholars increasingly term "weaponized interdependence" was not even raised in the EU Council's March 2026 conclusions.[23] Europe's growing engagement with economic security and statecraft reflects a belated recognition that the trade networks, supply chains, export controls, energy dependencies,

and financial flows that underpin prosperity can be converted into instruments of coercion and hybrid tactics. China's 2025 restrictions on exports of rare-earth elements, its coercive trade measures against Lithuania in 2021 after Vilnius allowed Taipei to open a Taiwan representative office in the country, and its strategic use of market access as diplomatic leverage exemplify how economic relationships that were once assumed to be mutually beneficial can be asymmetrically exploited.

Russia's weaponization of energy dependencies, laid bare by Europe's 2022 natural-gas crisis, offered the starkest example of such exploitation, yet similar dynamics are now playing out across technology supply chains, from advanced semiconductors to the critical minerals essential for Europe's green and digital transitions. The 2025 Nexperia dispute, in which a Chinese-owned chipmaker at the center of European automotive supply chains became the focal point of a cross-jurisdictional regulatory contest, compressed several of these dynamics into a single case: a company, a substrate technology, a supply chain, a legal order, and a geopolitical trajectory all made to turn on the same axis.[24]

The United States, ostensibly Europe's closest strategic partner, has become a source of comparable pressure. The Trump administration's embrace of tech billionaires as geopolitical interlocutors, its readiness to use technological and defense-industrial dependencies as leverage, and its skepticism of multilateral governance frameworks, through which Europe has traditionally exercised normative influence, have created a more uncertain strategic environment. Extensive U.S. tariffs on European goods have also intensified economic friction.[25] At the same time, Europe is still dealing with the longer-term pull effects of earlier U.S. industrial policy, especially the subsidy competition unleashed by the 2022 Inflation Reduction Act, which attracted firms and investments across the Atlantic. The extraterritorial reach of U.S. export controls that restrict European access to advanced semiconductors and AI components further shows that weaponized interdependence is not limited to adversarial states.

For European security planners, this means that threats stem not only from the antagonistic actions of China, Iran, or Russia but also from structural risks embedded in asymmetric dependencies on supposedly friendly providers whose strategic preferences may diverge significantly from European interests. In short, the lines between ally and adversary, and between commercial partner and geopolitical competitor, can no longer be treated as politically fixed.

The analytical challenge is that economic coercion and tech sovereignty are typically treated as separate policy domains. The European Commission's Anti-Coercion Instrument, the updated European Economic Security Strategy, and the EU's screening mechanisms for foreign direct investment all mark important advances in economic statecraft.[26] Yet, they operate largely in parallel with the EU's agenda for digital sovereignty rather than being integrated into a coherent strategic framework and operational logic. An ecosystems approach would hold that these domains are inseparable. Technological dependencies are themselves vectors of economic coercion and risks to strategic autonomy, which, in turn, degrades the conditions in which sovereign technology choices can be made.

Moreover, weaponized interdependence operates within and through information ecosystems. Economic coercion is most effective when paired with information campaigns that amplify public fears, sow division among target polities and allies, or shape elite perceptions of the costs and benefits of compliance. Beijing's combination of trade pressure on Lithuania with targeted messaging aimed at fracturing European solidarity on the status of Taiwan shows how economic and informational instruments reinforce one another in the same threat ecosystem.[27] A policy architecture that addresses economic statecraft in one institutional silo and information manipulation in another will systematically miss these synergies, ceding a strategic advantage to adversaries whose operational doctrines are designed to exploit such fragmentation and gray zones.

What this means in practice can be illustrated by the annulment of the 2024 Romanian presidential election. On a close reading of existing instruments, the case appears as a cluster of discrete problems addressed to separate entities: a FIMI incident for the European External Action Service (EEAS), a platform-compliance matter for the European Commission, an electoral-integrity concern for Romania as the member state, and a cyber dossier for the country's national intelligence services. Read through an ecosystemic lens, the same case describes a single feedback loop in which platform design choices, commercial amplification incentives, foreign-linked coordinated behavior, and the weakness of domestic information intermediaries jointly produced a constitutional crisis. In this respect, an ecosystemic reading of this case does not dissolve the existing policy and institutional instruments. It helps a desk officer tell which of them addresses which layer of the same problem, which tools are missing, and where the sequencing of strategic responses matters most.

The Romanian case could also be read as evidence that the EU has already mobilized several strands at once. It shows that Europe can bring together responses focused on platform oversight, electoral integrity, intelligence assessment, and FIMI under acute pressure. Yet, the episode also reveals the limits of a crisis-by-crisis model. What is still missing is a routine operating method for identifying a blueprint for the lead institution, sequencing instruments, and sharing evidence and expertise efficiently across policy silos. Such a method should also determine when dealing with an incident moves from platform risk management to a response focused on defending security, combating economic coercion, or protecting critical infrastructure. Consequently, ecosystemic coordination should entail a standing set of trigger criteria, playbooks, tools, and joint assessments, rather than another generic call for coherence and synergies.

A final caveat concerns the institutional scope of coordination between the EU and the North Atlantic Treaty Organization (NATO). The informational, infrastructural, cyber, and cognitive dimensions of European security increasingly run through NATO, which defines cognitive warfare as "the fight for cognitive superiority": aiming to influence, protect, or disrupt individual and group cognition to gain an advantage.[28] It is the weaponization of human mental processes to alter perceptions, behaviors, beliefs, and trust, often by targeting

democracies to weaken their cohesion and resilience. A coherent European approach will need to treat the EU-NATO interface as an integral part of the same ecosystem it aims to govern, rather than as a handover point between separate institutional regimes.

The institutional scaffolding already exists in parts. The European Centre of Excellence for Countering Hybrid Threats in Helsinki, the NATO Strategic Communications Centre of Excellence in Riga, and the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn have each accumulated significant domain expertise: on cross-sector scenario exercises, FIMI tradecraft, and cyber legal frameworks, respectively. The ecosystems task is to reconnect their outputs within a single analytical and operational picture, so that what these centers produce separately becomes legible as components of the same operating environment.

Bridging the Gap

If the EU and its members are serious about addressing hybrid threats, an ecosystems lens should translate into four concrete policy moves. First, the EU should devise a road map for comprehensive responses based on regular assessments of national information ecosystems and critical dependencies. Second, it should establish cross-domain coordination protocols with clear triggers, leads, operational ownerships, and escalation pathways across cyber, infrastructure protection, economic security, platform governance, FIMI, and democratic resilience. Third, the union should treat tech sovereignty and tech citizenship as mutually reinforcing, so digital infrastructures are governed as democratic public goods and not only as industrial or strategic assets. Fourth, the EU should identify and fund targeted interventions to enhance resilience where vulnerability mapping shows the highest risk of cascading.

This is not a plea for another layer of directionless coherence among instruments or institutions. It is a call for operational sequencing: who convenes, what evidence is shared, which instrument is activated first, which communities are protected, and how lessons feed back into policy action.

At the EU level, this should begin with a strategy for the information environment, jointly coordinated by the European Commission, the EEAS, and the Single Intelligence Analysis Capacity (SIAC), which combines civilian and military intelligence. In particular, this should involve SIAC's Hybrid Fusion Cell, which focuses on the analysis of hybrid threats. Meanwhile, EU member states would produce more detailed national assessments to feed into a shared analytical picture. This shift would allow the EU to move from a catalog of hybrid threats and risks to a clearer theory of where intervention is most needed.

Create a Road Map for Whole-of-Society Solutions

The EU is not starting from zero: Digital-citizenship education, media literacy, digital commons, e-government, citizen assemblies, civic-tech experiments, consultations on the Digital Services Act, and public-interest technology initiatives already form part of the European agenda.[29] However, these efforts have been modest, fragmented, underfunded, and overshadowed by the heavier machinery of tech sovereignty, platform regulation, and responses to FIMI.

An ecosystems approach would connect these initiatives to security and resilience policy without securitizing them. Once mapped, information ecosystems would provide an inclusive framework to give local journalists, educators, civil society, municipalities, researchers, and communities more consequential roles in resilience efforts. The aim is not performative consultation for its own sake but genuine citizen leverage over the infrastructures and incentives that shape democratic contestation and resilience.

Coordinate Threat Responses Better Across Silos

An ecosystems approach enables threat tracking across domains and silos, allowing the creation of cross-functional teams to respond to threats better. In many ways, whether adversaries openly articulate it this way or not, they are operating in a much more ecosystemic way than many democracies. For example, China's cognitive warfare investments—channeled through military-civil fusion strategies and the restructured People's Liberation Army Information Support Force, Cyberspace Force, and Aerospace Force, established in April 2024—represent a doctrinal integration of information, cyber, cognitive, and psychological operations that Europe has no institutional equivalent to counter.[30] Rogue actors, from ransomware collectives with state adjacency to private intelligence outfits that sell influence-as-a-service, add further layers of complexity.

Europe can learn from that integration without copying authoritarian doctrine. The goal is democratic coordination that clarifies responsibility, empowers communities, protects rights, and improves preparedness.[31]

An ecosystems approach would also enable cross-domain threat tracking by creating temporary, problem-specific cells around cascading vulnerabilities—for example, a combined cell for platform, cyber, and economic security and electoral integrity during an election period, or a maritime, energy, cyber, and information cell during an infrastructure incident in the Baltic Sea. These cells should be time limited, agile, tied to clear escalation thresholds, and

required to produce joint after-action reviews. This setup would avoid the familiar trap of broad coherence mechanisms that blur responsibility and drift into lowest-common-denominator language. The point is to improve decision quality in specific cases, not to build a permanent supersilo above existing silos.

Address Tech Sovereignty as Part of Democratic Security Governance

Assessing national information ecosystems can help quickly identify vulnerabilities that arise from dependencies on foreign technology and service providers.[32] In this respect, tech sovereignty should mean more than the nationality of suppliers or the competitiveness of European firms. It should also mean citizens' and public authorities' capacity to contest, audit, and shape the infrastructures that make up public life.

Working with friendly countries can, in turn, inform partnerships to address those vulnerabilities faster. This must be done in democratic terms—for example, by investing in cloud infrastructure, AI development platforms, and semiconductor capabilities while ensuring that these infrastructures are subject to transparent governance, public accountability, and democratic oversight. The lesson of the Starlink episode, the Nexperia affair, and the broader entanglement of European defense systems with U.S. technology platforms is that sovereignty without democratic governance is simply dependence with extra steps.[33]

Identify and Fund Interventions to Foster Resilience

Ultimately, over time, taking an ecosystems approach will help unlock what might constitute resilience in the information environment. The more national information ecosystem assessments are built over time, the better the information environment will be understood. This understanding can be accelerated with collective investments across EU members in shared research facilities.[34]

A critical caveat: The resilience in question is ecological, not engineering. Engineering resilience imagines a system returning to its prior equilibrium after a disturbance, which is exactly the wrong ambition for information ecosystems whose prior equilibriums were themselves fragile, extractive, or already captured. Ecological resilience instead asks which system states are worth sustaining, which transitions are worth absorbing, and which conditions require the ecosystem to reorganize itself around different structural arrangements.

Conclusion

The ecosystems approach has significant implications for how analysts and practitioners perceive security. It shifts the analytical focus away from domain-specific and individual threat vectors and toward the conditions that make entire ecosystems vulnerable to manipulation. It highlights the role of sociotechnical dynamics and what one of the present authors has called "information animals"—humans with all their cognitive biases, emotional vulnerabilities, and meaning-making impulses—as integral components of ecosystems rather than passive recipients of influence.[35]

Importantly, this perspective considers technology as an infrastructural factor that shapes the form of ecosystems—an internal rather than an external force. The approach considers the informational, cognitive, technological, and infrastructural aspects of modern threat landscapes simultaneously. If threats no longer respect domain boundaries and are cross-cutting, then analytical and institutional frameworks must also cross boundaries.

Taking this seriously also means accepting that information ecosystems are not simply found. They are sociotechnically co-produced by the regulatory choices, infrastructural investments, industrial initiatives, and political decisions that shape who can speak, on what terms, through which architectures, and with which forms of redress. In this regard, an ecosystems approach is not synonymous with a more holistic threat list. It is a claim about a more effective operational logic that determines where political agency lies and where responsibility for the conditions of democratic contestation must ultimately be assigned.

Used well, this approach should sharpen prioritization rather than dissolve it. The goal is not to make every problem part of one boundless map but to identify, using an escalation ladder, where policy interventions can most effectively reduce the most strategically significant vulnerabilities. For Europe, the practical test of an ecosystems approach is simple: whether it helps institutions see earlier, coordinate faster, use existing instruments better, and govern dependencies more democratically than the current hybrid toolbox allows.

Notes

1 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Potomac Institute for Policy Studies, 2007), https://www.comw.org/qdr/fulltext/0712hoffman.pdf.

2 Donald Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking," *Naval War College Review* 73, no. 1 (2020): 13–48, https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/4/.

3 "Council Adopts Conclusions on Advancing the EU's Capacity to Counter Hybrid Threats," Council of the European Union, March 16, 2026, https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/council-adopts-conclusions-on-advancing-the-eu-s-capacity-to-counter-hybrid-threats/.

4 "Council Adopts," Council of the European Union.

5 Richard Youngs, "Rethinking EU Digital Policies: From Tech Sovereignty to Tech Citizenship," Carnegie Europe, June 16, 2025, https://carnegieendowment.org/europe/research/2025/06/rethinking-eu-digital-policies-from-tech-sovereignty-to-tech-citizenship?lang=en&center=europe; and Richard Youngs, "Why Europe's Approach to Defending Democracy Is Failing," *Foreign Policy*, March 13, 2026, https://foreignpolicy.com/2026/03/13/europe-democracy-strategy-failing-polarization-centrism/.

6 Raluca Csernatoni, "Charting the Geopolitics and European Governance of Artificial Intelligence," Carnegie Europe, March 6, 2024, https://carnegieendowment.org/europe/research/2024/03/charting-the-geopolitics-and-european-governance-of-artificial-intelligence.

7 Raluca Csernatoni and Patryk Pawlak, "When AI Agents Attack: Autonomous Cyber Operations and Europe's Governance Gap," Carnegie Europe, July 6, 2026, https://carnegieendowment.org/europe/research/2026/07/when-ai-agents-attack-autonomous-cyber-operations-and-europes-governance-gap; and Raluca Csernatoni, "Can Democracy Survive the Disruptive Power of AI?," Carnegie Europe, December 18, 2024, https://carnegieendowment.org/europe/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai.

8 "Tackling AI Deepfakes and Sexual Exploitation on Social Media," European Parliament, January 15, 2026, https://www.europarl.europa.eu/news/en/agenda/plenary-news/2026-01-19/8/tackling-ai-deepfakes-and-sexual-exploitation-on-social-media.

9 Alicia Wanless, *The Information Animal: Humans, Technology and the Competition for Reality* (Hurst Publishers, 2025), https://carnegieendowment.org/research/2025/05/the-information-animal-humans-technology-and-the-competition-for-reality.

10 "'Disinformation Is One Problem Among Many in the Information Environment' - Interview with Alicia Wanless," EUvsDisinfo, July 1, 2024, https://euvsdisinfo.eu/disinformation-is-one-problem-among-many-in-the-information-environment-interview-with-alicia-wanless/.

11 "Amazon Web Services Outage Hits Airlines, Disrupting Check-Ins," CNBC, October 20, 2025, https://www.cnbc.com/2025/10/20/amazon-web-services-outage-hits-airline-websites-other-major-sites.html; "Amazon Outage 'Resolved' as Snapchat and Banks Among Sites Impacted," BBC News, October 21, 2025, https://www.bbc.com/news/articles/c20pgp3nx07o; "What We Know About the Massive Amazon Web Services Outage," CBC News, October 20, 2025, https://www.cbc.ca/news/canada/amazon-web-services-explainer-9.6946085; and "When Public Cloud Stumbles: Lessons from the AWS Outage and What They Mean for Healthcare," CloudWave, accessed June 4, 2026, https://gocloudwave.com/when-public-cloud-stumbles-lessons-from-the-aws-outage-and-what-they-mean-for-healthcare/.

12 Dennis Broeders et al., "Digital Sovereignty: From Narrative to Policy?," EU Cyber Direct, December 5, 2022, https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy.

13 Leticia Batista Cabanas and Elisabeth Heinz, "Mass Drone Warfare Is Europe's Rising Security Threat," Euronews, April 14, 2026, https://www.euronews.com/my-europe/2026/04/14/mass-drone-warfare-is-europes-rising-security-threat.

14 "Council Adopts," Council of the European Union.

15 Bruce D. Jones, "Seabed Zero: Baltic Sabotage and the Global Risks to Undersea Infrastructure," *Bulletin of the Atomic Scientists*, February 13, 2026, https://thebulletin.org/2026/02/seabed-zero-baltic-sabotage-and-the-global-risks-to-undersea-infrastructure/; and Miranda Bryant, "Finland Charges Tanker Crew Members with Sabotage of Undersea Cables," *Guardian*, August 11, 2025, https://www.theguardian.com/world/2025/aug/11/finland-accuses-tanker-crew-sabotage-undersea-cables-anchor.

16 Paul Kirby and Nick Thorpe, "Romania's Cancelled Presidential Election and Why It Matters," BBC News, December 6, 2024, https://www.bbc.com/news/articles/cx2yl2zxrq1o; and Mirel Bran, "Romania's Presidential Election Canceled over TikTok Disinformation Investigation," *Le Monde*, December 7, 2024, https://www.lemonde.fr/en/international/article/2024/12/07/romania-s-presidential-election-canceled-over-tiktok-disinformation-investigation_6735508_4.html.

17 Kunal Chaudhary, "The Cyberattack That Stole 280,000 Identities – and Showed How Easily We Can Be Duped," *Walrus*, October 16, 2025, https://thewalrus.ca/the-cyberattack-that-showed-how-easily-we-can-be-duped/.

18 Thomas Latschan, "Starlink: How Elon Musk's Company Influences Geopolitics," Deutsche Welle, February 15, 2026, https://www.dw.com/en/starlink-how-elon-musks-company-influences-geopolitics/a-75963477.

19 Raluca Csernatoni, "The EU's Hegemonic Imaginaries: From European Strategic Autonomy in Defence to Technological Sovereignty," *European Security* 31, no. 3 (2022): 395–414, https://doi.org/10.1080/09662839.2022.2103370.

20 Raluca Csernatoni, "Corporate Geopolitics: When Billionaires Rival States," *Strategic Europe*, Carnegie Europe, October 30, 2025, https://carnegieendowment.org/europe/strategic-europe/2025/10/corporate-geopolitics-when-billionaires-rival-states.

21 "EuroStack: Building Europe's Digital Future," EuroStack, accessed June 4, 2026, https://eurostack.eu/.

22 Csernatoni, "Corporate Geopolitics."

23 Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 42–79, https://doi.org/10.1162/isec_a_00351.

24 Suranjana Tewari, "Battle over Chinese Chip Maker Rocks Global Car Industry," BBC News, November 11, 2025, https://www.bbc.com/news/articles/cr43kyn9d6po.

25 Federica Di Sario, "The EU Wanted Stability. Trump's Tariff Fallout Brings Fresh Uncertainty," *Parliament Magazine*, February 27, 2026, https://www.theparliamentmagazine.eu/news/article/the-eu-wanted-stability-trumps-tariff-fallout-brings-fresh-uncertainty.

26 "European Economic Security," Council of the European Union, accessed June 4, 2026, https://www.consilium.europa.eu/en/policies/european-economic-security/.

27 Jessica Parker, "Lithuania-China Row: EU Escalates Trade Dispute with Beijing," BBC News, January 27, 2022, https://www.bbc.com/news/world-europe-60140561.

28 "Cognitive Warfare," NATO Science and Technology Organization, accessed June 4, 2026, https://www.sto.nato.int/document/cognitive-warfare/.

29 Youngs, "Rethinking."

30 Meia Nouwens, "China's New Information Support Force," International Institute for Strategic Studies, May 3, 2024, https://www.iiss.org/online-analysis/online-analysis/2024/05/chinas-new-information-support-force/.

31 Michael Berk, "Designing for Resilience: Building Institutions to Safeguard Information Ecosystems," International Institute for Democracy and Electoral Assistance, November 19, 2025, https://www.idea.int/publications/catalogue/designing-resilience-building-institutions-safeguard-information-ecosystems.

32 Alicia Wanless, Samantha Lai, and John Hicks, "Assessing National Information Ecosystems," Carnegie Endowment for International Peace, February 11, 2025, https://carnegieendowment.org/research/2025/02/assessing-national-information-ecosystems.

33 Csernatoni, "Can Democracy Survive?"

34 Alicia Wanless and Jacob N. Shapiro, "A CERN Model for Studying the Information Environment," Carnegie Endowment for International Peace, November 17, 2022, https://carnegieendowment.org/research/2022/11/a-cern-model-for-studying-the-information-environment.

35 Wanless, *The Information Animal*.

CARNEGIE
EUROPE

Rue du Congrès, 15
1000 Brussels, Belgium
CarnegieEurope.eu