idn brief

Abril de 2026

Ameaças Híbridas – Responder à Complexidade num Mundo Interconectado

DIRETORA
Isabel Ferreira Nunes
COORDENADOR EDITORIAL
Luís Cunha
CENTRO EDITORIAL
Filipa Teles
DESIGN EDITORIAL
Núcleo de Desenho do IDN - Paulo Jorge Pereira
PROPRIEDADE, DESIGN GRÁFICO E EDIÇÃO
Instituto da Defesa Nacional

ISSN 2182-5327
Depósito Legal 340906/12

Ameaças Híbridas – Responder à Complexidade num Mundo Interconectado

European Union governance and hybrid threats: integration, resilience, and strategic adaptation in a complex security environment

Evgenia Karatari
Deputy Head of the EU Situation Room
Crisis Response Centre (CRC)
European External Action Service

Introduction

In the rapidly evolving security environment, the European Union confronts new challenges that extend beyond traditional military threats. Hybrid threats are defined by their ability to combine military and non-military means, remaining below the threshold of conventional warfare. These threats exploit systemic vulnerabilities in democratic societies, targeting political cohesion, institutional integrity, and public trust.

Events such as Russia's annexation of Crimea in 2014, widespread disinformation campaigns, and the full-scale invasion of Ukraine in 2022 have accelerated the EU's strategic adaptation. These developments have exposed the limitations of fragmented national responses and reinforced the need for coordinated governance at the European level.

Hybrid threats as a concept

Hybrid threats are broadly understood as coordinated and synchronised actions designed to undermine democratic states while avoiding overt armed conflict. They integrate diverse tools – cyber operations, disinformation, economic coercion, and political interference – into a coherent strategy of disruption.

In the EU context, hybrid threats are particularly dynamic because they exploit the Union's multi-level governance structure. The division of competences between EU institutions and member states creates seams that adversaries can target. Moreover, the ambiguity and deniability that characterise the hybrid operations complicate attribution and delay response, undermining deterrence efforts.

The contemporary operational environment

Both state and non-state actors are carrying out hybrid activities characterised by increasing sophistication and frequency. These activities include foreign information manipulation and interference (FIMI), cyberattacks on critical infrastructure, electoral interference, economic coercion, and the weaponisation of migration flows.

The war in Ukraine illustrates the intersection between hybrid and conventional conflict. Prior to the 2022 invasion, Russia deployed extensive hybrid tactics – cyber operations, disinformation, and political destabilisation – demonstrating how hybrid strategies can prepare the ground for kinetic operations.

This environment is inherently transnational, requiring collective responses. No single member state possesses the full spectrum of capabilities necessary to counter hybrid threats effectively. This reality reinforces the EU's role as a coordinating and amplifying actor.

Evolution of the EU governance framework

The EU's response to hybrid threats has evolved significantly over the past decade. The 2016 Joint Framework on Countering Hybrid Threats marked a conceptual turning point, shifting from reactive crisis management to proactive resilience-building.

This framework was further developed through the 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities, and more recently through the Strategic Compass for Security and Defence (2022). Together, these initiatives structure EU action around four key pillars: situational awareness, resilience, response, and cooperation.

This governance model reflects the EU's hybrid nature as both a political and regulatory entity. Rather than relying primarily on military power, the EU leverages its strengths in coordination, regulation, and economic statecraft.

Institutional architecture and coordination

Effective governance of hybrid threats requires extensive coordination across institutional and policy boundaries. Within the European External Action Service (EEAS), entities such as the EU Intelligence and Situation Centre and its Hybrid Fusion Cell provide strategic analysis, while the EU Situation Room provides continuous monitoring, enhancing situational awareness, and supporting decision-making.

Cooperation with NATO is another cornerstone of EU strategy. The 2016 and 2018 Joint Declarations institutionalised collaboration on hybrid threats, cyber defence, and strategic communication. This partnership reflects a functional division of labour: NATO provides military capabilities, while the EU contributes civilian, regulatory, and economic tools.

Legal and regulatory instruments

A distinctive feature of the EU's approach is its reliance on regulatory instruments. Legislative initiatives such as the Digital Services Act (DSA), the Digital Markets Act (DMA), and the NIS2 Directive aim to strengthen digital resilience and counter disinformation.

Sanctions policy has also become a key component of the EU's hybrid toolbox. In response to Russian aggression, the EU has adopted extensive restrictive measures targeting financial systems, energy exports, and technology transfers. These measures illustrate the integration of economic statecraft into hybrid threat responses.

However, implementation remains dependent on member states, highlighting ongoing tensions between supranational coordination and national sovereignty.

Strategic communication and information resilience

Hybrid threats frequently target the information domain to polarise societies and undermine trust. The EU has developed dedicated capabilities to counter disinformation, including the EEAS StratCom Task Forces (East, Western Balkans, South, sub-Saharan Africa) and the EUvsDisinfo initiative.

Beyond reactive measures, the EU promotes media literacy, fact-checking networks, and partnerships with civil society. The Code of Practice on Disinformation exemplifies a co-regulatory approach, combining voluntary commitments with regulatory oversight.

Resilience as a strategic paradigm

Resilience has become the central organising principle of EU hybrid threat governance. Rather than attempting to eliminate threats entirely, resilience focuses on reducing vulnerabilities and enhancing the capacity to absorb and recover from disruptions.

This approach has been reinforced by recent crises, including the COVID-19 pandemic and the war in Ukraine, which exposed dependencies in supply chains, energy systems, and digital infrastructure. EU initiatives to diversify energy sources and strengthen critical infrastructure protection reflect this shift. However, resilience governance raises normative concerns. Measures aimed at enhancing security may expand state authority and affect civil liberties, necessitating careful balancing between effectiveness and democratic accountability.

Structural constraints and challenges

Despite significant progress, EU governance of hybrid threats faces persistent structural limitations. First, competence fragmentation limits centralised action, as security and defence remain primarily national responsibilities.

Second, divergent threat perceptions among member states complicate consensus. Eastern member states prioritise deterrence of Russia, while others focus on instability in neighbouring regions or migration-related challenges.

Third, internal challenges to the rule of law within some member states risk undermining the EU's credibility in defending democratic norms externally. Hybrid threat governance is thus closely linked to the Union's internal political cohesion.

The way forward

Looking ahead, hybrid threats are likely to intensify in both scale and complexity. Emerging technologies such as artificial intelligence, quantum computing, and space-based systems will create new vulnerabilities while expanding adversaries´ toolkits.

The EU is expected to deepen intelligence integration, enhance cyber capabilities, and strengthen partnerships with NATO and like-minded partners. At the same time, its regulatory influence will remain a key strategic asset in shaping global standards.

Conclusion

Hybrid threats represent a systemic challenge that transcends traditional security paradigms. The EU's response – anchored in integration, resilience, and regulatory innovation – demonstrates its capacity to adapt to a complex and evolving environment.

However, effectiveness ultimately depends on political unity, institutional coherence, and adherence to democratic principles. The governance of hybrid threats is not merely a technical exercise but a test of the EU's foundational values. Ensuring that security measures reinforce – rather than undermine – these values will be critical to the Union's long-term strategic credibility.

Disclaimer: The views expressed are purely those of the writer and may not in any circumstances be regarded as stating an official position of either the European External Action Service or the European Union.

The architects of our own ambush: how Allies co-produce hybrid threats

Roderick Parkes
Senior Researcher
NATO Defense College

The future of hybrid threats is usually discussed as a series of exotic technical problems. Yesterday, it was the manipulation of subsea cables, the weaponisation of forest fires, or deep-fake disinformation. Tomorrow, perhaps it will be the pharmacological sabotage of water supplies to induce psychological change, the remote manipulation of networked medical implants, or the automated harassment of citizens by turning their own administrative data against them. In Europe, this has become almost a form of strategic voyeurism. Foresight experts help Allies imagine new ways to be a victim, admiring the problem while failing to recognise their own role in producing it.

There is a tempting rabbit hole in modern foresight that involves dreaming up hyper-specific scenarios for every national anxiety. To the Portuguese, or any Ally on the Southern Flank, a focus on the exploitation of migration or natural disasters may feel like a visceral insight. Yet, imagine if every NATO nation pursued its own bespoke list of local vulnerabilities. The result would not be a strategy, but a cacophony of fears. Second-guessing the future is a sure way of exhausting resources. The best way to predict the future is to actively shape it, and this requires awareness of our own behaviour and responsibility. At present, there are certain common patterns of behaviour from the Alliance itself that invite opportunistic hostility.

Hybrid threats such as disinformation are only effective because the population - the centre of gravity in modern war - has been weakened. This weakness is not the sole result of a devious and creative adversary, but rather a co-production with our own governments. It is possible only because of the mistrust that Allied elites appear to have for their citizenry, a byproduct of the post-Cold War creation of a professionalised military and political class apart. To be useful, foresight must cease to be an elite exercise and turn a critical light on how the Alliance inadvertently creates vulnerabilities the more it becomes cut off from the society it is meant to protect.

In short, if we are thinking about the future of hybrid threats, we must be more aware of how we invite them through our own political and bureaucratic behaviour.

Stop framing the population as the problem

Political and military elites across NATO tend to frame our population as the problem. We describe them as vulnerable to hybrid threats because they are:

- dismissive of expert authority (post-rational),
- wary of the military instrument of power (post-heroic),
- and unaware of how economic dependencies exert political effect (post-civic).

This victim-blaming would hold more weight if NATO elites showed any great awareness of how we added to the problem. We like to say, for instance, that populations naively believed in the end of history and therefore do not even believe they face a threat, even when authorities tell them they do. In truth, it was the politicians who believed most heartily in the end of history. One needs only look at the Blair era in the 1990s to see the embrace of the idea that ideological competition had ended. Leaders failed to make the political case for anything, including defence.

As politicians became more technocratic, they forced technocrats to become more political – to provide "definitive" data for certain choices. Even as these choices backfired, for instance in the financial

crisis, they doubled down with the "TINA" (There Is No Alternative) logic. No wonder populations are today skeptical of authority and the supposed impartiality of government evidence. This is a rational response to government behaviour over the past 25 years.

Stop diagnosing a post-heroic citizenry

Public skepticism towards the use of military force is likewise an elite achievement. In the 1990s, political and military leaders accepted the diagnosis that Western societies had become post-heroic. Analysts such as Edward Luttwak observed the collapse of the Soviet army in Afghanistan and attributed it to demographic shifts; specifically, the lack of tolerance among Soviet mothers for the death of their only sons. This logic was promptly applied to shrinking, ageing Western populations.

Instead of scaling back the ambition of war or engaging society in the reality of its costs, Western elites entered new conflicts, which they presented as distant, bloodless, and won through technological shock and awe. The result was a military instrument overstretched as it was forced to achieve impossible goals. Our forces were first mired in so-called forever wars in Iraq and Afghanistan – attempting to translate high-tech kinetics into long-term liberalisation – before being repurposed as tools for domestic social transformation.

The legacy of this period is twofold: a population rightly skeptical of government calls for remilitarisation, and governments that seem almost grateful to be the objects of hybrid attacks. By staying below the threshold of open conflict, these attacks spare an elite from having to admit they no longer know how to ask their society for the use of force.

Recognise who is responsible for the weaponisation of dependencies

The narrowing of our political choices through economic dependency is, again, a product of elite design. When Allies expanded mutual dependencies through NAFTA and the Single European Act, it was societies that bore the political fallout. They experienced their countries' sudden vulnerability to economic trends beyond their borders, only to find their governments attempting to offload the burden of these gaps onto outside powers. To then decry these powers for "weaponising" those vulnerabilities is a case study in shifting responsibility.

Governments made the decisions, surrendered agency to markets, and then outsourced the consequences – first to external rivals and now to the voters themselves. This has produced a passive-aggressive approach to geopolitics. Allies are to blame for nothing; they are merely victims of implacable adversaries who exist only to exploit Western weakness. Meanwhile, populations are told to fend for themselves. It is the ultimate outsourcing of both responsibility and solutions and invites attack by opportunistic adversaries.

The common thread is the restoration of responsibility and agency

The way to reduce societies' vulnerability to hybrid threats is not to politicise expert advice, romanticise the warrior ethos, or retreat into the insulation of tariffs and industrial autonomy. These are reflexive gestures that only cement the mutual mistrust between voters and government while promising impossible solutions. Instead, elites must acknowledge their role in creating vulnerabilities and restore to the citizenry a meaningful part in resolving them.

An instructive case is the Swedish civil contingencies booklet. This is often cited as a model of effectiveness for a post-modern society – an example of government disciplining a population that had supposedly gone soft. The official narrative is a comfortable one for the establishment: when the booklet was released, Swedes complained of scaremongering, only to eat their words when the invasion of Ukraine proved the elites right and re-established the reign of expert reason.

In truth, the booklet was successful, because it provided citizens with practical instructions for the absence of a functional state – details as basic as meeting one's neighbours. By identifying their place in the solution, the population found a renewed interest in the problem. This was not the typical authority lecturing a passive audience about a threat without offering an answer; by providing a solution, the state helped its citizens remain awake to the problem.

The beginnings of a positive shift in NATO

The future of hybrid threats will not be decided in a technical cat-and-mouse game with a creative adversary. These threats are a co-production between Allied governing structures and opportunistic rivals. Elites can shape the future not by guessing the next exotic threat, but by correcting their own behaviour and restoring agency to the citizenry they serve.

A positive shift within NATO is becoming visible. There is a nascent pushback against our tendency to over-classify our actions. Moving sensitive elements into the public sphere – as with the nuclear exercise Steadfast Noon – treats the public as a partner rather than a liability. This is also evident in the effort to articulate the reality of long-drawn-out attritional warfare, rather than promising populations a quick, high-tech manoeuvre.

* This article reflects the author's personal opinion.

O Domínio Informacional como Teatro de Operações: desafios para a defesa nacional

Tiago Lapa
Professor Auxiliar, Departamento de Sociologia/Iscte

Num contexto estratégico cada vez mais marcado por ameaças híbridas, importa reconhecer que a segurança nacional vai muito para além do controlo do território físico ou da capacidade militar convencional. Hoje, o campo de batalha deslocou-se, em larga medida, para o domínio informacional e cognitivo, no qual perceções, emoções e narrativas se tornam instrumentos de poder e influência.

Esta transformação coloca-nos perante um paradoxo central. Por um lado, Portugal continua a apresentar níveis relativamente estáveis de segurança objetiva, aferidos por indicadores como os do Relatório Anual de Segurança Interna. Por outro, observa-se uma crescente sensação de insegurança entre os cidadãos, frequentemente dissociada desses mesmos indicadores. Portugal aparece, pois, como um país objetivamente seguro não só nos relatórios internos, mas também nos *rankings* internacionais. Contudo, subjetivamente, o país é sentido como inseguro ou sob ameaça por determinados segmentos da população, tendo essa perceção efeitos reais. Em muitos países, esta dissociação não é acidental. Ela resulta de um ecossistema informacional no qual a desinformação, as operações de influência e a amplificação algorítmica produzem efeitos cumulativos na forma como a realidade é percecionada.

A desinformação atua não tanto como causa autónoma, mas como um fator amplificador e multiplicador de fragilidades pré-existentes. Por um lado, explora vulnerabilidades psicológicas, como o viés de confirmação ou o efeito de verdade ilusória, que encontra eco no ditado popular de que uma mentira repetida mil vezes tende a ser tomada como verdade. Por outro lado, tira partido de vulnerabilidades estruturais, como a erosão da confiança nas instituições ou a crise de intermediação do jornalismo.

A segurança contemporânea depende tanto da gestão da informação como da gestão dos acontecimentos. Um incidente isolado pode adquirir um significado sistémico se for enquadrado narrativamente como sinal de colapso institucional. A realidade factual torna-se, assim, secundária face à realidade percecionada. Neste quadro, a Sociedade em Rede, tal como conceptualizada por Manuel Castells, não é apenas um contexto tecnológico, mas um novo paradigma estratégico. A informação deixou de ser suporte da ação política para se tornar o próprio terreno onde o poder se exerce. Estados que dominam fluxos informacionais, tecnologias digitais e capacidades de comunicação estratégica detêm vantagens decisivas não apenas em termos económicos, mas também em termos de segurança e legitimidade política.

É precisamente nesta interseção entre informação e poder que emergem as chamadas operações de influência, frequentemente integradas em estratégias de guerra híbrida. Estas operações não visam necessariamente destruir infraestruturas ou neutralizar forças adversárias, mas antes moldar perceções, fragmentar a coesão social e corroer a confiança nas instituições. O seu objetivo não é a vitória imediata, mas a degradação progressiva da resiliência societal.

Este tipo de conflitualidade coloca um desafio particularmente complexo às democracias liberais. Ao contrário de regimes autoritários, que podem controlar diretamente o fluxo informacional, as sociedades democráticas assentam num sistema de liberdades que constitui simultaneamente a sua maior força e a sua principal vulnerabilidade.

É neste ponto que se coloca a questão do equilíbrio entre a salvaguarda de direitos fundamentais, como a liberdade de expressão, e a necessidade de assegurar a segurança nacional. A liberdade de expressão é um pilar fundamental do Estado de direito democrático, consagrado constitucionalmente, mas pode ser limitada quando entra em colisão com outros direitos

ou com interesses públicos relevantes, como a segurança ou a integridade do sistema democrático. Contudo, a tentação de resolver o problema da desinformação através de restrições legais excessivas encerra riscos significativos. Uma resposta centrada exclusivamente na regulação pode conduzir a efeitos contraproducentes, nomeadamente à erosão da própria liberdade que se pretende proteger. Pode ainda alimentar narrativas de censura e reforçar a desconfiança nas instituições, agravando o problema que procura resolver.

Em contrapartida, a ausência de respostas eficazes cria um vazio rapidamente ocupado por atores que mobilizam o espaço informacional para fins estratégicos. As sociedades de informação enfrentam uma dificuldade estrutural em responder a formas de conflitualidade que operam abaixo do limiar da guerra convencional, num espaço ambíguo entre paz e conflito. Perante este dilema, torna-se evidente que a resposta não pode ser unidimensional. Exige uma abordagem integrada que combine três níveis de intervenção.

Em primeiro lugar, a nível estratégico, é fundamental reconhecer a soberania informacional como um pilar da segurança nacional e europeia. Tal implica investir em capacidades de monitorização de operações de influência, reforçar a transparência algorítmica no quadro regulatório europeu e desenvolver políticas públicas que integrem a literacia mediática como componente estrutural da defesa nacional.

Em segundo lugar, ao nível operacional, as instituições devem adotar uma postura comunicacional mais proativa. Num ambiente onde o vazio informativo é rapidamente preenchido por desinformação, a rapidez, clareza e credibilidade da comunicação institucional tornam-se determinantes. Estratégias como o *prebunking*, que consiste em estratégias preventivas, ou de "inoculação", que visam preparar cognitivamente os indivíduos para reconhecer e resistir à desinformação, por exemplo, através da antecipação de narrativas falsas e da exposição prévia a técnicas de manipulação, podem revelar-se eficazes.

Em terceiro lugar – e possivelmente o ponto mais decisivo – a nível societal, é imperativo reforçar a literacia mediática dos cidadãos. A resiliência de uma democracia depende, em última instância, da capacidade crítica da sua população. Num ecossistema informacional saturado, a capacidade de distinguir entre informação credível e manipulada torna-se uma competência cívica essencial.

A segurança no século XXI é inseparável da qualidade do ambiente informacional. A desinformação não destrói infraestruturas, mas corrói o tecido social, molda perceções, polariza sociedades e fragiliza a legitimidade das instituições. Neste contexto, a defesa nacional ultrapassa os meios tradicionais, exigindo também políticas de comunicação, educação e regulação orientadas para a proteção do espaço informacional.

Se a guerra híbrida tem nas perceções o seu principal campo de ação, então a resposta passa por fortalecer os cidadãos, tornando-os mais resilientes à manipulação e mais capazes de participar de forma crítica na vida democrática. A soberania informacional afirma-se, assim, como uma condição essencial para a preservação da liberdade, da segurança e da própria democracia.

Rise of authoritarianism, conflicts, technologies, divisions, and the use of hybrid threats

Hanne Dumur-Laanila
Analyst at Hybrid CoE.

Eginhards Volans
Senior analyst at Hybrid CoE.

Hybrid threats are on the rise as state and non-state actors increasingly rely on kinetic and non-kinetic asymmetric means to disrupt, destabilise, and affect their adversaries' decision-making[1]. Predominantly discussed and experienced in the Euro-Atlantic space, hybrid threats have become a truly global phenomenon, likely to remain in the news headlines for years to come. While the escalating nature of hybrid threats seems to be well established, the drivers and enablers behind them remain relatively underexplored or contested. This article aims to provide insights into why recent years have seen a surge in hybrid threats and what can be done to stop the trend from escalating further.

[1] Hybrid threats, as defined by the Hybrid CoE, are harmful, often combined activities that are planned and carried out with malign intent, used to undermine a target, such as a state or an institution, through various means, such as, but not limited to, information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force, etc.

Where hybrid threats thrive

As concluded by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), hybrid threats are carried out primarily by actors with authoritarian or totalitarian views of power[2]. As the number of authoritarian regimes increases, so does the use of hybrid threats. Today, authoritarian regimes have overtaken democracies as the most prevalent form of governance, while democracies have experienced erosion, with anti-democratic political actors consolidating power, weakening democratic institutions, and rising social unrest[3]. Consequently, established authoritarian regimes such as China are eager to promote their own socio-political model as a viable alternative to global audiences[4].

Hybrid threats are further reinforced by authoritarian regimes adopting increasingly hostile and risk-tolerant foreign policies, driven by the need for external threats, necessary for the regime's survival and domestic control. Russia, in particular, has cultivated a militarised ideology enforced through systemic indoctrination, total censorship, aggressive propaganda, and repressive legislation that demonises democratic values and calls for an inevitable clash between authoritarian and democratic worlds in which hybrid threats are increasingly useful[5].

On the other hand, the number of military conflicts has effectively doubled in recent years and has also contributed to the use of hybrid threats, as they have become integral to modern warfare[6]. Whether it is India and Pakistan launching global disinformation campaigns in May 2025; Iran blocking the Strait of Hormuz as a means of economic coercion against the US-Israeli partners; the use of armed proxies in the Sudan civil war, or the M23 incursion into the DRC; or Russia using the Israel-Hamas war as a pretext for driving divisions in Europe – hybrid threats are present in the majority of contemporary conflicts[7].

Hybrid threats have also been enhanced by the rapid evolution of emerging technologies, such as AI, which has become integral in tactics like cyber and information operations, making them more cost-effective and adaptive[8]. Similarly, advancements in drone technology have prompted the use of drones as deniable tools to disrupt infrastructure, test boundaries, exert psychological pressure, and influence decision-making[9]. Technologically advanced actors such as China have leveraged advances in space technology to enhance their hybrid threat capabilities in the space domain[10]. Furthermore, large technology companies

[2] Georgios Giannopoulos, Hanna Smith, and Marianthi Theocharidou, The Landscape of Hybrid Threats: A Conceptual Model (Public Version) (Luxembourg: Publications Office of the European Union, 2021), 15, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf.

[3] As concluded by the Varieties of Democracy project, at least 71% of the world's population lives under autocracies. Overall, there are fewer democracies than autocracies, with democracies becoming the least common regime type worldwide and reaching their lowest level of economic power in the last 50 years. See: https://v-dem.net/.

[4] Lydia Khalil, Peter Woodrow, James Paterson, and Robert Kaufman, "Understanding Democratic Erosion", Lowy Institute, August 2025, https://interactives.lowyinstitute.org/features/democratic-erosion/#intro; Niva Yau, "A Global South with Chinese characteristics", Atlantic Council, 13 June 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-global-south-with-chinese-characteristics/.

[5] Aleksandr Golts, The Land of Victorious Militarism – Militaristic Indoctrination in Russia, SCEEUS Report No. 6 (Stockholm: Centre for Eastern European Studies, 9 May 2025), https://sceeus.se/en/publications/the-land-of-victorious-militarism-militaristic-indoctrination-in-russia/; Dima Kortunov and Julian G. Waller, "The DNA of Russia: Ideology and Patriotic Education in Wartime Russia", Russia.Post, 30 October 2024, https://russiapost.info/politics/dna_of_russia; "Disrupted, Throttled, and Blocked. State Censorship, Control, and Increasing Isolation of Internet Users in Russia", Human Rights Watch, 30 July 2025, https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation; Andrei Soldatov and Irina Borogan, "Browser History: The Kremlin's Newest Weapon", CEPA, 30 July 2025, https://cepa.org/article/browser-history-the-kremlins-newest-weapon/.

[6] Mathew Newman, "A "new normal": tracking the rise of global conflict", Lowy Institute, 23 December 2025, https://www.lowyinstitute.org/the-interpreter/new-normal-tracking-rise-global-conflict.

[7] Nabiya Khan, Kaushik Raj, and Zenith Khan, Inside the Misinformation and Disinformation War Between India and Pakistan (Washington: Centre for the Study of Organized Hate, 2025), 3, https://www.csohate.org/wp-content/uploads/2025/05/Report_CSOH_Inside-the-Misinformation-and-Disinformation-War-.pdf; Jack Watling, "Iran's Hormuz blockade is its most powerful card against Trump and Israel. It won't back down easily", The Guardian, 16 March 2026, https://www.theguardian.com/commentisfree/2026/mar/16/iran-strait-of-hormuz-blockade-trump-israel; Johan Sävström, "Gulf states' proxy war exacerbates conflict in Sudan", The Nordic Africa Institute, 7 February 2025, https://nai.uu.se/stories-and-events/news/2025-02-07-gulf-states-proxy-war-exacerbates-conflict-in-sudan.html; "M23, Rwanda's Proxy to Secure Control of Congolese Wealth", The Oakland Institute, https://www.oaklandinstitute.org/report/shafted/m23-rwandas-proxy-secure-control-congolese-wealth; Maria Shamrai, "How Russia uses the Israel-Gaza Crisis in its disinformation campaign against the West", ICCT, 8 December 2023, https://icct.nl/publication/how-russia-uses-israel-gaza-crisis-its-disinformation-campaign-against-west.

[8] Elena Grossfeld, "If You Can't Beat Them, Steal: Russia's AI Strategy", King's Centre for the Study of Intelligence, 3 November 2025, https://kcsi.uk/kcsi-insights/if-you-cant-beat-them-steal-russias-ai-strategy; Julien Barnes, "China Turns to A.I. in Information Warfare", The New York Times, https://www.nytimes.com/2025/08/06/us/politics/china-artificial-intelligence-information-warfare.html.

[9] Christofer Lawers, "The Threat Posed by Commercial First-Person View (FPV) Unmanned Aerial Vehicles (UAVs) Modified by Asymmetrical Warfare Actors" in The Co-Evolution of Technology and Warfare, ed. Tracey German, Fotios Moustakis, and Andrew N. Liaropolos (Routledge Studies in Conflict, Security and Technology, 2025), 41-56.

[10] Conlan Elis, Theodora Ogden, and James Black, China and space: How spa-

have themselves become both key enablers and targets of hybrid threats, as entire segments critical to national security, such as communications infrastructure and microchip manufacturing, are often controlled by them[11].

Finally, there has been an issue of counterproductive policies being adopted by the very democracies targeted by hybrid threats. At a time when hybrid threat actors, such as Russia, have intensified cyber operations and allocated record-high levels of funding to propaganda, some governments have halted counter-cyber operations, reduced funding for pro-democracy media initiatives, and reduced social media content moderation[12]. Furthermore, scaling back on global financial integrity, transparency, anti-corruption, and anti-money-laundering initiatives has likely facilitated the ease of conduct of hybrid threat operations and evasion of detection[13].

Strategic recommendations

Against the backdrop of rising authoritarianism, a decline in democratic values, military conflicts, rapid technological advancement, and counterproductive decision-making, hybrid threats have become more sophisticated and expansive than ever before. To address this worrying trend, comprehensive and coordinated responses are required.

First, democracies must be strengthened internally, alongside a proactive promotion of their values abroad, including engagement with the populations of authoritarian states. Second, enhanced national security capabilities should be developed and clearly signalled to deter potential aggressors while sanctions are consistently imposed sanctions on those who violate international law. Third, greater oversight of large technology companies is needed, alongside efforts to leverage them and their technologies in countering hybrid threats. Finally, Euro-Atlantic political establishments must foster a shared understanding that hybrid threats transcend political and geographical divisions and pose a threat to all societies and governments.

ce technologies boost China's intelligence capabilities as part of hybrid threats (Hybrid CoE, October 2024), 7, https://www.hybridcoe.fi/wp-content/uploads/2024/10/20241021-Hybrid-CoE-Paper-21-China-and-space-WEB.pdf; Sandra Erwin, "China's space ambitions hit a new gear", Space News, 18 November 2025, https://spacenews.com/chinas-space-ambitions-hit-a-new-gear/.

[11] Geert van der Klugt, "Big tech conquers internet infrastructure, wipes out telco providers", Techzine, 18 January 2022, https://www.techzine.eu/news/infrastructure/71312/big-tech-conquers-internet-infrastructure-wipes-out-telco-providers/; Josh Mahan, "Who Builds Data Centers?", C&C Wavetech, 21 March 2025, https://cc-techgroup.com/who-builds-data-centers/; Herman Quarles van Ufford, "When the chips are down: Nexperia, Europe and the US-China trade and tech war", ECFR, 21 October 2025, https://ecfr.eu/article/when-the-chips-are-down-nexperia-europe-and-the-us-china-trade-and-tech-war/.

[12] Dan Milmo, "Russian cyber-attacks against Nato states up by 25% in a year, analysis finds", The Guardian, https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds; Antonia Langford, "Kremlin Pours Record Sums into State Propaganda", Kyiv Post, 3 October 2025, https://www.kyivpost.com/post/61421; Jasper Jackson, "Trump is giving Russian cyber ops a free pass", The Bureau of Investigative Journalism, 7 March 2025, https://www.thebureauinvestigates.com/stories/2025-03-07/trump-is-giving-russian-cyber-ops-a-free-pass-and-putting-western-democracy-on-the-line; "USA: How 'Defunding' the US Agency for Global Media sacrifices freedom of expression for millions", Article 19, 21 March 2025, https://www.article19.org/resources/usa-how-defunding-the-us-agency-for-global-media-sacrifices-freedom-of-expression-for-millions/; Richard Luscombe, "Trump administration moves to deny visas to factcheckers and content moderators", The Guardian, 5 December 2025, https://www.theguardian.com/us-news/2025/dec/05/trump-administration-us-visa-crackdown.

[13] "Trump Administration Scales Back Beneficial Ownership Reporting Requirements Under the Corporate Transparency Act", Simpson Thatcher, 31 March 2025, https://www.stblaw.com/about-us/publications/view/2025/03/31/trump-administration-scales-back-beneficial-ownership-reporting-requirements-under-the-corporate-transparency-act; "Pausing Foreign Corrupt Practices Act Enforcement to Further American Economic and National Security", The White House, 10 February 2025, https://www.whitehouse.gov/presidential-actions/2025/02/pausing-foreign-corrupt-practices-act-enforcement-to-further-american-economic-and-national-security/; "Trump's First 100 Days in Office Raise Doubts Over US Commitment to FATF", ACAMS, 28 April 2025, https://www.acams.org/en/news/trumps-first-100-days-in-office-raise-doubts-over-us-commitment-to-fatf.

idn Instituto da Defesa Nacional

Calçada das Necessidades, 5, 1399-017
Lisboa
Tel +351 211 544 700
idn.publicacoes@defesa.pt