

Almanach #16

Commentary by Andro Gotsiridze

War Beyond the Battlefield: Subversion and the Challenge of Democratic Resilience

The opinions and conclusions expressed are those of the author and do not necessarily reflect the views of the EU Awareness Centre.

© [2026] EU Awareness Centre. All rights reserved.

10 November 2026

War Beyond the Battlefield: Subversion and the Challenge of Democratic Resilience

Recent bomb threats disrupting European flights, cyberattacks targeting civilian infrastructure and reports of unidentified drones raise questions about the strategic significance of seemingly isolated incidents. This commentary examines how operational disruption can become an instrument of subversion, exploiting vulnerabilities in human security to undermine public confidence, economic stability and political will. Focusing on Russia's confrontation with Europe, it explores how sustained insecurity and financial losses may generate political pressure and potentially weaken support for Ukraine. While distinguishing strategic motives from verified attribution, the analysis argues that democratic resilience depends on protecting public trust, social cohesion and political decision-making autonomy.

Several incidents across Europe in recent weeks have raised questions extending well beyond their immediate security implications.

In early November, a wave of false bomb threats disrupted dozens of passenger flights across Europe, prompting diversions, military escorts and heightened airport security. No explosives were found, and investigators have yet to establish who was responsible.

Around the same period, cyberattacks targeting supermarket refrigeration systems disrupted operations across several European countries, causing food spoilage and financial losses. A pro-Russian hacking group claimed responsibility for attacks during the November wave, although the claim remains unverified, as Paris Match reported. A similar attack in France in October was formally attributed to an Iranian cyber unit. Different actors may pursue different objectives, but the vulnerabilities they exploit and the wider consequences of disrupting civilian infrastructure can be remarkably similar.

What, then, connects these incidents? Perhaps nothing. Yet their potential strategic significance deserves examination, particularly against the background of Russia's confrontation with Europe.

An earlier incident offers a revealing parallel. In September 2025, Copenhagen Airport suspended operations for nearly four hours following reports of unidentified drones. A subsequent police investigation found insufficient evidence to confirm their presence, although it could not rule them out. The disruption nevertheless illustrates how the perception of a threat can produce significant operational consequences even without a confirmed attack.

The geographical scale is equally significant. Between April and mid-October 2026, a joint investigation coordinated by the European Broadcasting Union documented hundreds of suspected hybrid incidents across 17 European countries, including sabotage attempts, airspace violations and activities involving locally recruited operatives.

Unlike sabotage targeting arms production facilities or logistics routes supplying Ukraine, where the immediate objective may be to disrupt military assistance, the significance of attacks on civilian infrastructure may lie less in their operational consequences than in how the resulting fear, economic insecurity and disruption of everyday life can undermine human security, public confidence and political decision-making.

Contemporary conflict extends far beyond conventional military operations. Economic activity, critical infrastructure and everyday life have become increasingly exposed to hostile interference, allowing states to pursue strategic objectives without formally entering into armed conflict. Against this background, subversion has acquired renewed significance.

Subversion is not simply disinformation or political manipulation. It exploits vulnerabilities within an adversary's political and social systems to undermine institutional effectiveness, social cohesion and the capacity to sustain independent political decisions. Its effectiveness lies partly in turning a society's own characteristics against it.

Once dependent on intelligence networks and covert influence, subversion has been transformed by digital technologies. Social media, advanced analytics and artificial intelligence enable hostile actors to identify vulnerabilities and amplify narratives at unprecedented speed and scale. Cyber operations extend these capabilities into economic activity, public services and critical infrastructure.

The objective is not necessarily to destroy military capabilities or inflict substantial physical damage. Undermining public confidence, generating uncertainty and weakening political will may prove equally consequential. Even relatively minor disruptions can acquire disproportionate political resonance, while repeated incidents may allow hostile actors to test NATO countries' responses and identify vulnerabilities.

In this respect, Clausewitz's logic of compelling an adversary to submit to one's will remains relevant in today's digitally connected world, where economic disruption, psychological pressure and cyber operations can undermine political will without necessarily resorting to military force.

In Russia's confrontation with Europe, a plausible strategic objective is to weaken European political will to sustain support for Ukraine - and potentially bring that support to an end.

Defeating European armies on the battlefield would present Russia with a formidable challenge, but Moscow does not need such a victory to pursue its strategic objectives. Having failed to achieve a rapid victory in Ukraine, and facing sustained Ukrainian resistance supported by European assistance, Russia may instead seek to raise the economic and political costs of that support, exploiting divisions within European societies and testing the determination of their governments.

Russian sabotage operations across Europe have targeted critical infrastructure and economic activity, causing financial losses, service disruptions and additional security costs, as documented by IISS and S&P Global Market Intelligence. A recent CSIS study further highlights how modern conflicts increasingly expose private companies to geopolitical risks, forcing corporate leaders to weigh operational security, financial losses and broader strategic considerations.

Repeated disruptions and financial losses may prompt businesses to seek government intervention, particularly where corporate interests and national security priorities diverge. Whether sustained disruption could eventually lead affected businesses to call on European governments to reconsider their support for Ukraine remains a hypothesis worth monitoring, rather than an established outcome.

However, such pressure would not necessarily produce the outcome Moscow seeks. If managed correctly, through effective crisis response, credible public communication and political leadership, these incidents could instead strengthen public resolve, reinforce social cohesion and increase support for a firmer response to Russian aggression.

Sabotage becomes an instrument of subversion when its purpose extends beyond operational disruption to erode political confidence and decision-making autonomy. Financial losses, interrupted transport and manufactured insecurity may produce cumulative political effects if employed as part of a sustained campaign.

Such effects would be consistent with Russia's strategic interest in undermining European support for Ukraine. That does not establish Russian responsibility for the incidents concerned. A plausible motive is not evidence of attribution, and similar operational patterns do not demonstrate a coordinated campaign. Premature conclusions may themselves amplify the uncertainty and mistrust that hostile influence operations seek to create.

Democratic societies are particularly exposed because their strengths — open media, political competition, public accountability and the legitimate influence of business interests — can also be exploited by hostile actors. Yet restricting democratic openness cannot be the answer. The challenge is to preserve these characteristics while reducing susceptibility to manipulation and coercion.

The immediate implications extend beyond conventional security measures.

For security and intelligence services, assessing individual incidents solely by their operational consequences is no longer sufficient. National hybrid-threat assessments should also incorporate human security indicators, including disruptions to essential services, perceived safety, economic insecurity and public trust in institutions. This would help governments see how seemingly limited incidents can create broader societal vulnerabilities and potentially affect political decision-making.

For businesses operating critical infrastructure, geopolitical threats must become an integral part of corporate risk management. Business continuity planning, crisis exercises and cooperation with public authorities are essential, particularly when commercial disruption may carry broader political and national security consequences.

For governments and democratic societies, resilience also depends on effective crisis communication, institutional credibility and social cohesion. Independent research institutions and civil society can contribute through evidence-based analysis, countering disinformation and communicating uncertainty responsibly. A human security perspective is equally important, as vulnerabilities affecting individuals and communities can create opportunities for political coercion even when state institutions remain operational.

Ultimately, democratic resilience cannot be measured simply by the ability to prevent every attack. It must also be measured by the capacity to absorb disruption, preserve public confidence and maintain political independence despite sustained pressure.

For European democracies, the challenge is therefore not merely to protect their infrastructure, but to ensure that fear, uncertainty and economic disruption do not determine their political choices — including their decisions about supporting Ukraine.



Andro Gotsiridze *is a Georgian intelligence and cybersecurity expert with extensive experience in intelligence operations, national security, and corporate security.*