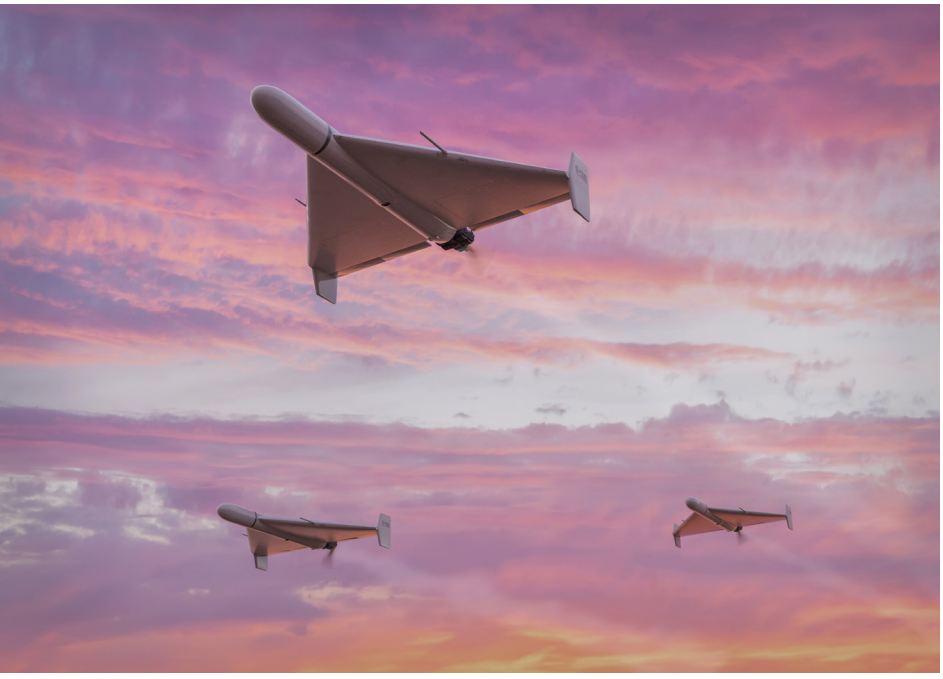
INSIGHT REPORT

Russia-Ukraine conflict spillover into NATO territory: Implications for European operations

OCTOBER 2026

KEY JUDGEMENTS



- We assess that the most plausible pathways for spillover of the Russia-Ukraine conflict involve accidental, misidentified or otherwise ambiguous incidents that create uncertainty over intent and responsibility.
- Poland remains the most plausible location for conflict spillover due to its proximity to Ukraine and role as a logistics hub supporting the Ukrainian capital Kyiv. However, similar escalation dynamics could emerge elsewhere along NATO's eastern flank, including Romania, Finland and the Baltic states.
- For countries further removed from the conflict, spillover is more likely to occur in the form of a significant escalation in hybrid activity.
- For most organisations, the most likely impact would stem from heightened uncertainty and a deteriorating security environment. Indications of the latter include operational disruption, cyber threats, travel restrictions and supply chain pressures. The severity of organisational impacts would depend less on the incident itself than on how the authorities respond to it.

OVERVIEW

Increased tensions between Russia and other European states have contributed to a more volatile security environment in parts of Europe during 2026 to date. Germany publicly attributed an attempted drone attack overnight on 4-5 August at Leipzig/Halle Airport (LEJ, Germany) to Russia and announced a series of diplomatic and security measures in response. The incident prompted expressions of solidarity from NATO and European leaders, alongside renewed commitments of support for Ukraine and action to counter hostile Russian activities in Europe.

These developments do not indicate an imminent conventional conflict between NATO and Russia. However, they reinforce a broader European perception that the continent faces an acute and persistent threat of hybrid activity. In this context, these are hostile activities below the threshold of conventional armed conflict, including cyber operations, sabotage, disinformation, electronic interference, espionage and proxy actions. As tensions rise, so too does the risk of unintended escalation, particularly from miscalculation, operational error, hybrid activity and/or conflict spillover.

We assess that the most plausible pathway to a wider European security crisis is not a deliberate Russian attack on NATO territory, but an incident where the intent is disputed or unclear. For countries located further from the conflict, spillover is more likely to occur via cyber activity, sabotage, infrastructure disruption and other forms of hostile hybrid activity than direct military action. Such an event could generate political pressure for a response, increase military readiness measures and alter the operating environment for organisations across Europe.

For most organisations, the principal risk stems from uncertainty and disruption rather than direct military action. Potential consequences include changes to government security measures, transport disruption, heightened cyber threats, increased concern among employees and pressure on critical infrastructure and logistics networks.

This Insight Report focuses primarily on the more plausible escalation scenario of a military-related incident affecting a NATO member state bordering Ukraine, Belarus or Russia. Such countries face greater exposure to cross-border military activity, creating a higher likelihood that an incident could generate uncertainty regarding Russian intentions and increase the risk of escalation. Poland is used as the principal illustrative example due to its proximity to the conflict and strategic importance in supporting Ukraine.

For countries located further from the conflict, spillover is more likely to occur through cyber activity, sabotage, infrastructure disruption and other forms of hostile hybrid activity than through direct military action.

ASSESSMENT

The security environment

[illegible]

[illegible]

1. [illegible]
2. [illegible]
3. [illegible]

[illegible]

Get in touch to have access to the full report

[illegible]

Illustrative escalation scenario: Poland

[illegible]

[illegible]

1. [illegible]
2. [illegible]

INSIGHT REPORT

Europe - October 2026

Get in touch to have access to the full report

Implications for organisations

Get in touch to have access to the full report

Figure 1 - Anticipated business impacts by category

[illegible]

Get in touch to have access to the full report

RECOMMENDATIONS TO MANAGERS

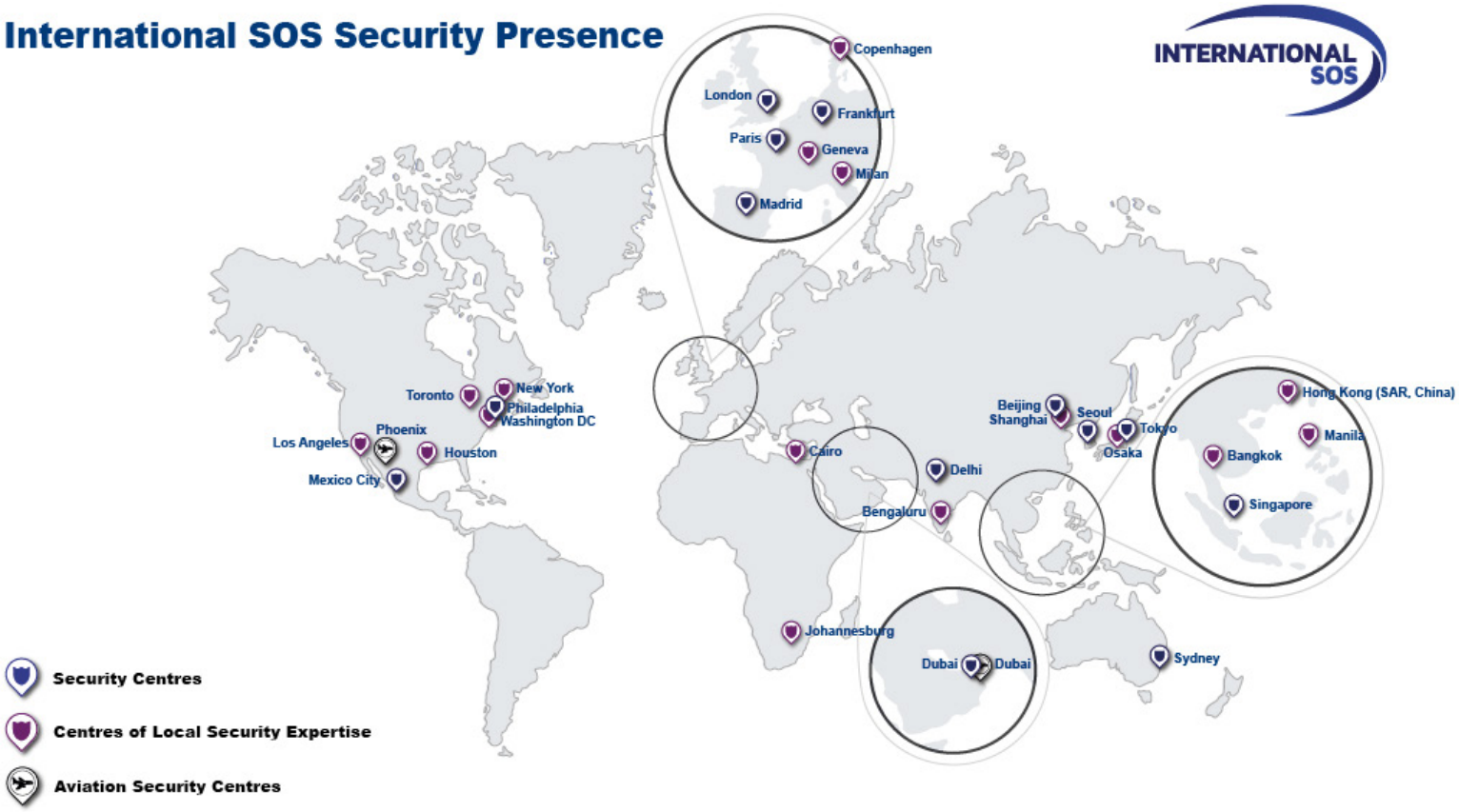
Illustrative organisational response triggers

Get in touch to have access to the full report

Get in touch to have access to the full report

ACTIONABLE INSIGHTS AND UNPARALLELED SERVICES

International SOS and its network of partners combine the world's leading security and medical risk specialists. With access to more than 3,200 security specialists led by our 200 dedicated security experts based in our Assistance Centres and offices around the world, we provide a comprehensive suite of integrated security risk services for the global workforce and managers tasked with keeping people safe, secure and healthy. We deliver timely, actionable security intelligence, analysis, advice and on-the-ground assistance.



For follow-up questions about the assessments or recommendations in this Report, please call your nearest Assistance Centre.

Copyright © International SOS, 2026. All rights reserved. Reproduction in whole or in part is prohibited without the prior consent of the Company.